Sécurité Globale
HORIZONS STRATÉGIQUES
8
Nouvelle série

Dossier

CYBER-CHAOS ET SÉCURITÉ NUMÉRIQUE

- Aujourd'hui, demain : la cyber-sécurité, par les plus grands experts francophones
- Sécurité informatique et usager de base
- La NSA, mauvais génie du cybermonde
- Démons et merveilles du « prédictif »

Géopolitique

- La sécurité des ouvrages hydrauliques dans un monde dangereux

Chroniques

- La prison, les malfaiteurs : déconstructions
- Faits & idées criminologiques
- Tribune libre : lutte anti-crime dans les banlieues

Editions ESKA

Introduction

De la cyber-jungle au cybermonde

Xavier RAUFER

Quatre thèses fondatrices de la cyber criminologie[1]

- *Diagnostic 1* - Dans l'ensemble «cyber-crime», crime domine. Scruter le monde cyber-criminel révèle qu'il n'a rien inventé d'original. Dans leur milieu et jusqu'à présent, les cybercriminels se bornent à reproduire les variantes de la criminalité physique.

- *Diagnostic 2* - La cybercriminalité ne baissera pas par plus encore de haute technologie, mais par *décision* politique. Dans ce domaine, une fuite en avant type blindage-et-canon provoquerait un désastre analogue à celui de l'inepte guerre *high-tech* d'Irak.

- *Traitement, 1* - Il faut au cybermonde un code de la route comme, en son temps, la société de l'automobile suscita le sien. Un code conçu et imposé par une coalition de nations puissantes, dans l'espoir raisonnable qu'il s'imposera mondialement. Autre image pour l'indispensable superstructure normative : celle de la tour de contrôle.

- *Traitement, 2* - Le code de la route vaut pour tout véhicule, luxueux ou modeste : de même, seul un code du cybermonde sanctionnera-t-il vraiment les prédateurs, financiers maraudeurs, géants du net, etc., qui, aujourd'hui, le pillent impunément ou exploitent ses usagers.

CRIME et monde numérique - le problème aussi mondial qu'énorme - d'abord, par la taille de ses acteurs de premier plan :

- Facebook a 1,7 milliard d'utilisateurs qui en moyenne, passent quelque 50 minutes par jour sur ses sites et applications ;
- Autre titan de l'Internet, Apple a vu en 2015 son chiffre d'affaires atteindre 234 milliards de dollars.

Ainsi, tout ce qui circule, invente, construit, vend, paie, etc., sur la planète s'inscrit désormais dans un cybermonde qui, en matière de sécurité et sans doute pour longtemps encore, ressemble fâcheusement à la Banque de France - moins les coffres forts.

Cour des miracles et Piste Ho-Chi-Minh à la fois, le cybermonde est presque sans défense ; trop souvent, bandits, pirates, espions, saboteurs, etc., s'y ébattent, volent et pillent à leur aise. Or comme il est toujours aussi ardu d'attribuer précisément une attaque dans le monde numérique, les cybermalfaiteurs se rient d'une répression semblable à l'Arlésienne d'Alphonse Daudet, qu'on attend toujours - mais ne vient jamais. Cela bien sûr, ces malfaiteurs adorent.

Or trop souvent, les Etats et grands groupes font comme si la menace était secondaire ou anodine. Ils assurent le minimum syndical, une rustine ici, un sparadrap là, espérant que le méga-piratage, ou le super-sabotage, attendra la prochaine élection ou le prochain bilan. Quand au commerce de la cyber-sécurité, il tend à s'enfermer dans une logique d'ingénieurs, considérant - idée Ô combien fausse - qu'un souci technique se corrige par plus de technique encore. Ce dans le mépris de tout ce qui n'est pas codeur. Pour ces preux chevaliers du cybermonde en effet, l'usager moyen de l'informatique et de l'Internet n'est qu'une sorte de simplet, défini en langue *Geek* par la formule PICNIC (*Problem In Chair, Not In Computer*).

Cependant, les signes avant-coureurs d'un cyber-chaos aggravé se multiplient ces derniers mois. En voici quelques uns de préoccupants pour des domaines stratégiques : défense, monde des entreprises, finance, crime organisé, etc.

■ **DÉFENSE** : en août 2016, on apprend que la célèbre et effrayante NSA (*National Security Agency*) s'est fait voler d'ultrasecrets outils de piratage, conçus par l'unité d'élite de l'agence, le TAO (*Tailored Access Operations*, opérations d'accès sur-mesure). Un groupe de hackers nommé *Shadow Brokers* (en référence aux personnages d'un jeu vidéo) organise sur le site *Pastebin* une ironique et humiliante vente aux enchères ; qui veut acheter les jouets du service secret le plus secret au monde ? Dans la communauté américaine du renseignement en effet, ses rivaux prétendent que NSA signifie «No Such Agency»...

Les mois suivants, la réalité éclate : vieux en fait de 16 ans ce piratage de la NSA est (à l'instant...) le vol de documents secrets le plus massif de l'histoire ; immensément plus que le vol d'Edward Snowden en 2013.

On parle de «plusieurs terabytes de données» volées. Pour les Béotiens, un terabyte équivaut au contenu en volume d'environ un million de livres.

Là resurgit le bon vieux facteur humain - celui qui affecte nos cyber-ingénieurs eux-mêmes… Car le pillard présumé (qui travaillait pour TAO) est un *geek* parmi d'autres, un peu poivrot, se prenant pour James Bond, perdu dans le grand jeu numérique et voulant sauver le monde du cyber-diable. Des «montagnes de documents» sont retrouvés par le FBI dans le foutoir de sa vie personnelle, entre sa voiture, un logis en grand désordre et une baraque à outils…

■ **GAFA & co. : victimes eux aussi.** GAFA, ce sont les quatre titans de l'Internet : Google, Apple, Facebook et Amazon. Libertaires d'idées et de pratiques, ces géants sont à leur tour victimes des pirates. Le 21 octobre 2016 : *Amazon, eBay, Spotify, Airbnb, Netflix, Paypal, Twitter* ; les jeux en ligne de *Playstation* et de *XBox* ; rayon médias, *CNN*, le *New York Times*, le *Boston Globe*, le *Financial Times*, le *Guardian*, sont inaccessibles des heures durant ; mondialement, des millions (minimum) d'usagers sont privés d'accès à ces serveurs majeurs.

L'attaque informatique géante qui les frappe tous cible en fait DYN, société prestataire dans le domaine des DNS (*Domain Name System*). L'attaque a été menée par un «Bot» exploitant les failles de sécurité des objets connectés (caméras de surveillance, téléviseurs, etc.). Relais possibles d'attaques majeures, ces objets connectés sont désormais des millions (voitures autonomes… domaine de la santé… maisons «intelligentes», etc.) et à ce jour, nul antivirus ne les sécurise vraiment.

Qui sont les pirates ? Comme d'usage les «experts», officiels ou privés, pataugent et n'en savent en réalité rien. Ils pressentent cependant que la généralisation du *Cloud* et des *Smartphones* n'arrangera pas les choses… Déjà, *Yahoo*, *MySpace*, *LinkedIn* ont subi de massifs pillages : environ 1,5 milliard de comptes «braqués» par des pirates de l'été 2015 à l'été 2016. (*Yahoo* : ± 500 millions de comptes piratés ; *MySpace*, 427 millions ; *LinkedIn*, 117 millions).

Que cherchent les pirates dans ces pillages ? Des comptes «pépites», où figurent : identifiants, adresses de courriels, mots de passe, adresses postales ; mieux, des dates d'anniversaires et références bancaires. Ce luxe de données autorise des arnaques sur mesure, personnalisées, pouvant viser des particuliers, des entreprises ou des institutions.

Pour les grands groupes, notamment dans le domaine de l'énergie, la sécurité numérique tourne au cauchemar stratégique. En 2018, les seules sociétés pétrolières investiront 1, 87 milliard de dollars pour se protéger.

■ **FINANCE, classique ou Bitcoin** : fonctionnant depuis 1977, la plateforme financière SWIFT (*Society for Worldwide Interbank Financial Telecommunication*) est

le réseau sanguin de la finance mondiale. Or en février 2016, la Banque d'Etat du Bangladesh a subi un braquage de 81 millions de dollars - la banque étant ciblée plus que la plateforme Swift elle-même, mais à travers celle-ci. De par le monde, d'autres structures financières ont subi des pertes lors d'attaques analogues ; d'abord en Asie (Japon, Philippines, Vietnam), mais aussi aux Amériques (Nord, Latine), en Europe et en Australie.

A l'automne 2016, la City de Londres s'alarme de la forte augmentation des attaques visant les institutions financières britanniques : on en comptait 5 pour toute l'année 2014 ; il y en a eu 75 de janvier à septembre 2016. Toutes cibles confondues et pour l'année 2015, le Royaume-Uni a subi environ 2,5 millions de *cybercrimes*, dont 250 000 seulement ont fait l'objet de plaintes auprès de la police.

Côté Cybermonnaies, on note l'inquiétant enthousiasme du WEF-Davos, notoire agent d'influence de la DGSI (Davos-Goldman-Sachs-Idéologie), pour la technologie *Blockchain*, issue de l'architecture *Bitcoin*. Inquiétude car par le passé, la DGSI, le WEF Davos et consorts ont toujours dédaigné toute stratégie sérieuse visant à protéger la planète des prédations financières.

Ce, alors que les monnaies, ou devises, virtuelles sont toujours aussi fragiles. Début août 2016, on apprend le piratage de *BitFinex*, l'une des grandes plateformes mondiales d'échanges de Bitcoins : 60 millions de Bitcoins «braqués» par des auteurs (comme d'usage...) inconnus et introuvables. Autre pillage en juin 2016 : la plateforme DAO (*Decentralized Autonomous Organization*) se fait voler environ 50 millions de dollars d'une autre monnaie digitale nommée «Ether». Rappelons que déjà en 2014, l'importante plateforme *Mt.Gox*, de Tokyo, avait vu «disparaître» 119 756 Bitcoins (valeur lors du vol, 72 millions de dollars).

■ **CRIME ORGANISÉ** : celui-ci pille et pirate la finance numérique, surtout en usant de deux armes/techniques/méthodes. Le «siphonage» des DAB (Distributeurs automatiques de billets) et le *Ransomware*, qui voit un pirate verrouiller l'accès à un ordinateur ou à des données personnelles puis les libérer contre rançon (d'usage payée en *Bitcoins* sur un compte exotique.

En mai 2016 dans 17 préfectures du Japon, Tokyo inclus, d'importants clans yakuza (Yamaguchi Gumi, Kobe Yamaguchi Gumi, Dojin-Kai, Inagawa-Kai, Sumiyoshi Kai et Godda-Ikka), associé à des pirates-experts, multiplient les retraits de 100 000 yen (maximum autorisé) sur des cartes de paiement trafiquées, à l'origine émises par la *Standard Bank of South Africa*. Butin total : 1,8 milliard de yens (1, 75 million de dollars).

Côté *Ransomware*, spécialité du monde russe, des entreprises cybercriminelles comme «Petya» et «Misha» se spécialisent dans ces formes de «kidnapping numérique»,

devenues un véritable *business* parallèle, avec son marketing, la création de «franchises» et la vente d'outils criminels spécifiques (avec modes d'emploi vidéo, etc.).

■ **DEMAIN, l'avenir proche** : Les cyberguerres ne sont plus une lointaine fiction. Dans la constamment excellente *New York Review of Books* ((29/09/2016) Un expert observe : «Les cyber-armes sont furtives. Ni explosions ni boules de feu : comme tout en informatique, elles se composent de 0 et de 1 ; on s'en sert pour infiltrer en douce des machines individuelles, ou des réseaux entiers. Frappant précisément, elles peuvent paralyser d'immenses infrastructures, brouiller les signaux de l'ennemi, interrompre des communications ; aussi, riposter à des attaques, et les neutraliser, avant même qu'elles ne débutent». Selon Edward Snowden, les Etats-Unis ont mené dès 2011 213 de ces cyber-attaques - qui sont bien d'ordre militaire : «chaque fois que *Stuxnet* était déclenché (virus censé paralyser les centrifugeuses iraniennes produisant de l'uranium de qualité militaire) un officier de la CIA se tenait derrière l'opérateur de l'ordinateur et lui donnait l'ordre d'attaquer».

Enfin, les capacités criminelles de l'intelligence artificielle («*machine learning*»), domaine de recherche majeur de l'informatique de demain. Bientôt, vous risquez d'entendre au téléphone une voix familière : proche, collègue... La «voix» sera aux mains de pirates voulant vous piller, vous manipuler, vous induire à faire ceci, vous pousser à interrompre cela. Le logiciel existe déjà : c'est donc pour bientôt.

Ainsi - comme les criminologues l'observent de longue date - logiciels et algorithmes ne sont qu'une moderne version de la langue d'Esope, meilleure et pire des choses à la fois. Mais si la sagesse grecque des origines l'enseignait déjà voici vingt-cinq siècles, des ingénieurs un peu perdus dans le champ du seul calculable l'entrevoient à peine...

Annexe : La criminalité de l'Internet aux Etats-Unis en 2015, selon le FBI

(Il y a quelque 270 millions d'usagers de l'Internet aux Etats-Unis début 2016, sur une population de ± 323 millions d'habitants)

Statistiques générales

Niveau fédéral (national), Etats-Unis : environ 1,08 milliard de dollars de préjudices constatés pour l'année de référence ; 288 012 plaintes reçues, dont 127 145, suite à une perte financière (perte moyenne : $ 8 421).

Infractions-Internet signalées

- par le biais de réseaux sociaux : 19 967
- par usage des monnaies virtuelles : 1 920

Type d'infractions signalées *(10 000 victimes ou plus)*

- Défaut de paiement ou de livraison : 67 375 *infractions signalées*
- Surfacturation (419, *nigérianes*) : 30 885
- Vol d'identité : 21 949

- Enchères truquées/fraudes : 21 510
- Vol de données personnelles : 19 632
- Fraudes à l'emploi : 18 758
- Extorsion : 17 804
- Fraudes à la carte de paiement : 17 172
- Phishing & analogue : 16 594
- Fraudes à l'avance sur paiement : 16 445
- Intimidation et violence : 14 812
- Escroquerie sentimentale ou à la confiance : 12 509
- Escroquerie à la qualité : 11 832
- Escroquerie dans l'immobilier : 11 532

Plus de cent millions de dollars US de préjudice

- Usage frauduleux d'emails dans les affaires (escroquerie «au président» ou à l'israélienne : 264,3 millions de dollars de préjudice
- Arnaque à la confiance ou aux sentiments : 203,4m.$
- Arnaque au paiement ou à la livraison : 121, 4m.$
- Arnaque à l'investissement : 119,2m.$

Sources

Xavier Raufer «Cyber criminologie» - CNRS Editions, 2015

US Department of Justice - BBI 2015 Internet Crime Report

New York Review of Books - 27/10/2016 «They've got you, whenever you are»

New York Times International - 25/10/2016 «As artificial intelligence evolves, so does its criminal potential»

Le Parisien - 23/10/2016 «Piratage massif de sites Internet : quand les objets connectés attaquent»

Le Parisien - 22/10/2016 «Ce qui se cache derrière la cyberattaque massive qui a touché Internet»

New York Times International - 20/10/2016 «Trove of stolen data is said to include top secret US hacking tools»

Le Figaro - 18/10/2016 «Cybersécurité : pourquoi les entreprises sont de plus en plus vulnérables»

Reuters - 14/10/2016 «Banks are hiding their cyber-attacks»

GNT (Site) - 13/10/2016 «Cyber menace : le crime organisé s'empare du ransomware»

Yomiuri Shimbun - 4/10/2016 «6 yakuza crime groups implicated in Y. 1.8 Billion ATM scam»

Le Point - 2/10/2016 «Réseau interbancaire : les attaques de pirates informatiques continuent»

New York Review of Books - 29/09/2016 «US cyber weapons our demon pinball»

Libération - 18/08/2016 «La NSA dans le viseur de Shadow Brokers»

New York Times International - 15/08/2016 «Bitcoin technology seen going global»

New York Times International - 4/08/2016 «Hacking at Bitcoin exchange»

Note

[1] «Cyber criminologie», Xavier Raufer, CNRS-Editions, 2015.

Démons et merveilles du « prédictif » : une bonne fois pour toutes...

Xavier RAUFER

Notre monde physique est balisé et connu – mais l'autre, le numérique ?

La seconde guerre mondiale s'achève et Paul Valéry pré-voit ainsi le monde à venir : «Toute la terre habitable a été de nos jours reconnue, relevée, partagée entre les nations. L'ère des terrains vagues, des territoires libres, des lieux qui ne sont à personne, donc l'ère de libre expansion est close. Plus de roc qui ne porte un drapeau ; plus de vides sur la carte ; plus de région hors des douanes et hors des lois ; plus une tribu dont les affaires n'engendrent quelque dossier et ne dépende, par les maléfices de l'écriture, de divers humanistes lointains dans leurs bureaux. *Le temps du monde fini commence* (...) Le monde auquel nous commençons d'appartenir, hommes et nations, n'est qu'une figure semblable du monde qui nous était familier. Le système des causes qui commande le sort de chacun de nous, s'étendant désormais à la totalité du globe, le fait résonner tout entier à chaque ébranlement ; *il n'y a plus de questions finies pour être finies sur un point.*»

En d'autres termes, Valéry décrit un «*Nomos* de la terre» l'ordre spatial de la Grèce antique réinventé par Carl Schmitt : «Le *Nomos* règle, pour tous les citoyens de la ville, le partage de ce qui leur est destiné»[1] ; telle est l'œuvre de Némésis, déesse qui répartit entre les dieux et les hommes.

Le monde fini de Valéry dure quarante ans : dès 1985, l'ordre planétaire se fragmente et le *Nomos* tourne au *Chaos,* quand apparaissent les «zones grises» au Sud du monde. Encore n'est-ce rien à côté de ce qui attend la Terre - car peu après, apparaît un continent (numérique) vierge et inconnu, le cybermonde.

Et quel continent ! Ecoutons son chantre, John Perry Barlow, président de la *Electronic Frontier Foundation* (et parolier du groupe de rock californien les *Grateful Dead)* : «Un continent si vaste qu'il pourrait

être illimité… Un monde nouveau que toute notre avidité n'épuisera sans doute jamais ; offrant plus d'opportunités qu'il n'y aura jamais d'entrepreneurs pour les exploiter ; un lieu où les malfaiteurs ne laissent nulles traces ; où, mille fois volés, les biens appartiennent toujours à leurs légitimes propriétaires… Où seuls les enfants se sentent vraiment chez eux…» («Déclaration d'indépendance du cyberespace», Davos, 1996).

Retour à aujourd'hui.

Frénétiquement, le présent cybermonde cherche à se comprendre lui-même. Il est vrai que ce monde-là exige de l'ordre : ses concepteurs, architectes et opérateurs viennent d'un milieu mathématique stable, ordonné et prédictible, où 2+2 font toujours 4 ; depuis toujours, le calculable est d'ailleurs leur refuge face au chaos du monde.

Notre «société de l'information» (car reposant sur l'informatique) se sait toujours incapable de maîtriser (modéliser) l'incertitude, l'à-venir. Mais elle éprouve l'urgent besoin d'annoncer (au moins) qu'elle le pourra bientôt ; que cette invention est imminente. Rien de neuf sous le soleil : dans cette société nerveuse et fragile, tout autant qu'à l'âge d'Aristote, l'angoisse de l'homme tient toujours à ce qu'il ne connait pas, ne peut connaître, l'heure de sa propre mort.

Même fictivement, cette société doit donc prétendre qu'elle surmontera l'angoisse humaine de l'avenir ; qu'elle maîtrisera demain l'in-calculable. D'où son obsession de la modélisation, de l'intégrale compréhension du monde. Chaque jour, le cyber-tam-tam annonce ainsi une nouvelle «solution» prédictive… l'état de santé… la finance… la toxicomanie… la police… nous verrons cela plus bas ce que vaut ce «solutionnisme».

En attendant, le *Big data* est la panacée ! Détecter et analyser les signaux émis par les hommes… Découvrir et exposer les *patterns* (modèles) inconnus : il y a tant de données inexploitées, partant desquelles élaborer ces modèles inédits. Tout analyser, tout corréler, tirer du sens de tout : telle est la présente ivresse du cybermonde. Elle est compréhensible : le champ de la prédiction ne grandit-il pas à mesure qu'on exploite de nouvelles bases documentaires, elles-mêmes toujours plus interconnectées ? Les limites à l'analyse prédictive ? On ne les voit pas.

D'où vient ce tam-tam prédictif ? De Silicon Valley

Quand elle se protège, la «société de l'information» se rue systématiquement sur des défauts et failles des systèmes numériques, sans trop s'interroger sur le système lui même. Dans une culture d'ingénieurs, le système est bon s'il fonctionne bien. Nul besoin de s'interroger sur ses fins dernières ; d'aller voir derrière le décor. Or bien sûr, les origines et finalités du cybermonde proviennent de la fort suspecte «Silicon Valley». Toutes deux méritent qu'on y aille

voir de près ; faute de quoi, on posera *ad vitam æternam* des rustines sur le pneu crevé - sans chercher qui a répandu des clous sur la route.

Or dès l'origine, Silicon Valley fréquente - avec délices - des espions, des mafieux, des fraudeurs - on l'a même créée pour ça : «Silicon Valley a grandi comme une filiale de l'armée et du renseignement des Etats-Unis» (cf. Malcomson, bibliographie). On verra plus bas que même des icônes du cybermonde ont trempé là-dedans.

Cela, les agents du système l'admettent eux-mêmes : « S'ils travaillent dur à inventer nos futures technologies, nombre d'entrepreneurs de Silicon Valley négligent les risques sociaux, légaux, éthiques et sécuritaires que leurs créations font courir à la société… Les développeurs de Facebook ont longtemps eu comme slogan 'Foncez et cassez tout au passage' (*move fast and break things*), devise affichée au siège de la société… Marc Zuckerberg renchérissant : «si vous ne cassez jamais rien, vous ne foncez pas assez»[2].

Et les mafieux ? Ils sont là dès la décennie 1970. Alors, les réseaux d'ordinateurs communiquent par les lignes téléphoniques existantes, grâce à une gamme de tons sonores (chuintements caverneux familiers aux usagers des premiers modems) Vite, de jeunes aveugles apprennent le sens et l'usage de ces tons - donc les failles du système : ces proto-*hackers* communiquent ainsi gratuitement entre eux, mais peuvent aussi écouter les échanges des autres. Ils s'associent alors à des *Geeks* pour fabriquer de primitifs modems et ouvrir à des clients cet univers en marge. Vendues une centaine de dollars, ces «petites boîtes bleues» piratent le système téléphonique Bell qui en vaut, lui, des centaines de milliards.

Qui fabrique ces petites boîtes bleues ? Dans les garages d'anonymes villas californiennes ou dans des clubs libertaires nommés «*People' computer company*» ou «*Homebrew computing club*», de juvéniles et chevelus post-Hippies ; parmi eux, Steve Wozniak et Steve Jobs, futurs fondateurs d'Apple (Wozniak l'avoue, 4/10/1984, dans un discours à la *Colorado School of Mines*). Qui sont les principaux clients des «petites boîtes bleues» ? Les mafieux de Las Vegas («When Vegas mobsters bought blue boxes from phone freaks», *Esquire*, cf. bibliographie).

Pour conclure sur ce point, mieux vaut garder en mémoire qu'outre ces douteuses fréquentations, que «Silicon Valley» qualifierait sans doute d'erreurs de jeunesses [3], la «Vallée» possède aussi, aujourd'hui encore, sa propre idéologie libertarienne *bottom-up*, auto-organisation d'individus, d'actions et de marchés, qu'elle juge bien supérieure aux vieilles régulations paternalistes *top-down*, avec leurs contraignants cadres, catégories et conventions. Le «gouvernement algorithmique» dont rêve «Silicon Valley» est fondé sur l'exploitation des justes données du *Big data*, sur ce que chaque individu fait en

réalité ; donc, dit-»elle», moins paternaliste, injuste et déformant que nos actuelles institutions.

Ce cyber-pouvoir est défini - de façon plutôt inquiétante - par Mme Antoinette Rouvroy, chercheuse en philosophie du droit à l'Université de Namur *(Mediapart, 25/05/15, bibliographie)* : «Nourri essentiellement de données brutes, signaux infra personnels et a-signifiants mais quantifiables ; opérant par configuration anticipative des possibles plutôt que par règlementation des conduites ; et ne s'adressant aux individus que par voie d'alertes provoquant des réflexes, plutôt qu'en s'appuyant sur leurs capacités d'entendement et de volonté». En bon français : de la manipulation à grande échelle.

Silicon Valley, des sommets du lyrisme utopique à la froide réalité du fric

Chers ingénieurs, journalistes et politiciens, ne croyez pas à la neutralité du système numérique (soi-disant voué au bien de l'humanité) rayonnant depuis la Silicon Valley. Ne croyez pas ces cyber-évangélistes et leur chatoyant «solutionnisme». Car la superstructure de Silicon Valley n'est finalement qu'un copier-coller de la bourgeoisie, dont Karl Marx a ainsi défini le rôle historique : « Partout où elle a conquis le pouvoir, elle a foulé aux pieds les relations féodales, patriarcales et idylliques... Elle a noyé les frissons sacrés de l'extase religieuse, de l'enthousiasme chevaleresque, de la sentimentalité petite-bourgeoise dans les eaux glacées du calcul égoïste» *(Manifeste du Parti communiste)*.

Et ce qu'elle propage en prétendant lutter contre le paternalisme d'hier n'est rien d'autre que son paternalisme à elle, celui qu'elle imposera demain : «bons» comportements, modes vertueuses, bienséance, hygiénisme, etc.

Retour à aujourd'hui : tout mesurer, tout contrôler, tout prévoir par *le Big data* ? Difficile et surtout, dangereux. Creusons. Sous les grandes proclamations, on trouve : domination, prédation, exploitation, aliénation, opacité. L'addiction numérique, aussi ; la fascination pour les écrans et les algorithmes - tout sauf neutres et perpétuant plutôt les inégalités sociales - on le verra plus bas. Enfin, une idéologie vide de politique, un idéal d'administration *high-tech*, de gestion anonyme et un management d'autant plus féroce qu'il affecte d'être *cool*.

Concluons en citant Michael Brenner, l'un des rares intellectuels américains à toujours «*think out of the box*» (*cf. bibliographie*) : «Oubliez les slogans *(de Silicon Valley, Ndl'a)* et leurs utopies inouïes ; oubliez le culte de l'électronique *high-tech* ; oubliez les fascinantes nouvelles frontières. En fin de compte, le seul étalon du succès, de la réputation, du statut social - et des plaisirs que procurent l'argent et l'amour - sont prosaïquement : le fric et les *stock-options*».

Silicon Valley dit «prédire» – mais qu'est-ce que la prédiction ?

«Prédire» est le maître-mot de Silicon Valley. Et policer la cité est clairement stratégique. Mais qu'est-ce que prédire en matière stratégique ? Tout remonte à la seule grande bataille navale de la première guerre mondiale, celle du Jutland[4]. Au bilan, la *Royal Navy* constate que son artillerie n'a mis que 3% de coups au but. Pour préciser les futurs tirs («*fire control program*»), la *Navy* forme des calculateurs. Ces premiers «*computers*» humains (de là provient le mot) doivent pré-voir, anticiper les mouvements des navires ennemis, en intégrant l'inertie temporelle, du moment où l'obus (ou la torpille) est tiré à celui où il touche sa cible.

Même problème lors de la seconde guerre mondiale. Encore neutre en 1940, Washington veut cependant aider la Grande-Bretagne lors du «Blitz» ; il ne peut livrer des armes - mais fournir de la matière grise aux amis est licite. La science balistique américaine optimisera donc l'artillerie anti-aérienne britannique lors de la bataille de Londres. Pour cela, des statisticiens doivent anticiper l'évolution des bombardiers (vols en zigzag, décrochements, etc.) ; prédire leurs mouvements, pour tirer à coup sûr. Dans un champ d'action donné (d'où vient et où évolue l'avion), ils doivent deviner un comportement (où cet avion va).

Solution théorique : *l'anti-aircraft predictor model*. Un système de tir automatique couple des canons anti-aériens à des radars (qui existent déjà). Un ultra-rapide processus probabiliste (le «prédicteur») fournit des données pertinentes (partant de ce que montre le radar) ; le tir «anticipe» donc les mouvements de l'avion et l'abat, sinon à tout coup, mais bien plus sûrement qu'avant.

Norbert Wiener, mathématicien de génie et pionnier de la cybernétique, relève le défi. Sa mission (en anglais) : imaginer «*the mathematics of predicting the movements of hostile airplanes according to probability*»[5]. Avec son collègue Julian Bigelow, ils tentent de modéliser un ensemble de comportements, humains et mécaniques : que se passe-t-il quand un pilote veut éviter des tirs de DCA ? Peut-on comprendre et modéliser les fort complexes interactions homme-machine qui soudain s'opèrent ? La logique opérationnelle de l'esprit du pilote visé est à chaque fois différente, bien sûr. Mais, estime Wiener, l'esprit humain sous tension tend à agir répétitivement et est donc prévisible.

Une machine est donc construite pour stocker et croiser des données sur les possibles figures aériennes du bombardier en vol, les réactions du pilote et les modalités du tir, afin d'obtenir l'anticipation voulue. Le premier «*computer*» - non plus humain, mais *mécanique* - est né. Notons que comme son ancêtre biologique post-Jut-

land, il lui est assigné d'anticiper *à temps* un comportement humain.

D'une seconde à l'autre, la prédiction de la machine est étonnante de précision - mais inutile, car les obus des canons anti-aériens mettent 20 secondes à atteindre l'altitude du bombardier en vol. La prédiction exigée est donc à 20 secondes. Et là, échec irrémédiable. C'est impossible, quelle que soit la puissance de calcul asservie à cette fin. Norbert Wiener abandonne le projet *anti-aircraft predictor model* en janvier 1943.

Depuis et pour l'essentiel, on en est là. La prédiction *réelle* se heurte encore et toujours à la barrière du temps. Nous parlons ici de la *vraie* prédiction : pas de l'hypothèse hasardeuse qu'un individu fera ceci demain, du fait qu'il a fait cela hier. Genre *Amazon* : «ceux qui ont acheté tel livre ont aussi aimé...». Cela n'est en rien de la prédiction mais (en anglais) du «*wishful thinking*».

D'ores et déjà, ces rappels historiques montrent l'audace de prétendre «prédire» un crime, action complexe et d'usage secrète, soudaine ou bien ourdie de longue date et impliquant deux humains minimum - voire bien plus.

Prédire en puisant dans le Big data ?

«Silicon Valley» balaie ces objections en affirmant qu'aujourd'hui, tout a changé, du fait du *Big data*. Le progrès technologique a doté l'humanité d'un immense, peut être d'un illimité, vivier de données susceptibles de multiples réutilisations, sans rapport avec leur collecte initiale. L'informatique permet de capter, conserver et traiter ces données, puis d'y repérer des corrélations.

Ce stock disponible, dit «Silicon Valley», est un nouveau, et décisif, facteur de production ; c'est la matière première de demain. «Les algorithmes permettront de faire des prédictions sur la dangerosité des personnes ou leur probabilité de commettre un acte particulier, à partir des *Big data* et des corrélations que l'on peut y trouver», dit ainsi un thuriféraire de la *data science*. Nous y voilà.

Sont-elles précises, ces corrélations ? Non, mais leur multitude compense leur flou. Les prévisions faites à partir de ces données sont elles valides ? Pas forcément, mais dans la *data science*, les erreurs servent : dans un domaine précis de recherche, chaque nouvelle vague de calcul intègre et corrige les fautes précédentes. Ici, disent les *Data Scientists*, pas de corrélations fallacieuses : plus ça va, et plus les prévisions sont précises.

Comme méthode, la modélisation prédictive par voie mathématique-informatique exige un indispensable outil : l'algorithme. La méthode plus l'outil produisent à leur tour le logiciel, qui les associe pour un projet, ou dans un champ, précis. Voyons maintenant si ces divers cyber-ustensiles sont fiables et solides.

Prédire en modélisant – mais qu'est-ce qu'un «modèle» ?

D'abord, écartons ce qu'à l'heure présente, nul logiciel, modèle ou algorithme ne peut accomplir : aucun de ces outils numériques ne peut comprendre, moins encore créer, un concept. Aujourd'hui, nul programmeur ne sait transcrire en code un sarcasme, de l'argot ou un propos cynique.

Venons-en au modèle : il représente abstraitement (dans un ordinateur ou dans sa tête) un processus qui part de ce qu'on sait déjà, puis «prédit» des réponses, ou réactions, à divers cas ou situations. Sorte de maquette facile à comprendre, elle permet d'inférer des faits situés dans l'à-venir. Fatalement, le modèle simplifie un réel infiniment plus complexe : la carte n'est pas plus le territoire que le logiciel n'est la vie vécue d'un être humain.

Qui plus est, les logiciels permettant la *data-science* ne sont pas des forces neutres et inexorables (comme le vent ou les marées) ; ils ne tombent pas du ciel, mais reposent sur les choix effectués par de faillibles êtres humains. Ces «modèles» qui toujours plus guident nos vies et génèrent une crainte religieuse - voire pratiquent l'intimidation mathématique - ne sont trop souvent qu'un ensemble codé de préjugés, de biais et d'incompréhensions. Loin d'éclairer la réalité, ils peuvent finir par l'incarner, suscitant un pseudo-réel qui - miracle ! - justifie les résultats obtenus : on parle alors de modèle autoreproducteur.

Pourquoi ? Tout modèle repose sur le choix humain, conscient ou non, des données à considérer ou rejeter ; *toujours,* un codeur décide de ce qu'on y inclut. Un modèle n'est pas une radiographie, mais porte les opinions, priorités et jugements de valeur de son concepteur, si honnête soit-il. Pour Cathy O'Neil *(cf. bibliographie)*, un modèle est «une opinion nichée dans un ensemble mathématique»

Comment ? Quand on élabore un modèle et que manquent les données exactes à coder sur ce qu'on recherche vraiment, on use de données proches, faisant fonction de… Dans le champ du stratégique ou de la justice, choisir ces ersatz est bien sûr fort politique, voire idéologique.

Concrètement : voici un logiciel aidant la justice à prédire les risques de récidive. Intégrant une masse d'informations sur l'environnement humain et géographique d'un individu, ce logiciel assume forcément que ces faits tirés de son passé seront répétitifs. Or comme codifier des données anciennes n'invente *en rien* le futur, chercher dans ces données *passées* des éléments d'un verdict ne «prédit» rien, mais projette ce passé dans l'avenir.

Pour quel résultat ? Rappel : avant le krach de 2008, tous les modèles d'anticipation des risques financiers assumaient que l'avenir de Wall Street ressemblerait à son passé :

on a vu le travail… Bienvenue dans la «face noire du *Big data*».

Modéliser exige des algorithmes – mais qu'est-ce ?

La capacité algorithmique, c'est la «possibilité de produire, à partir d'un ensemble de données, une fonction calculable permettant de comprendre, caractériser, expliquer ou *prédire* l'état courant ou *futur* des données capturées». On parle ainsi d'algorithmes, de modèles, de technologies *prédictifs*. (cf. *Archives de philosophie du droit*, bibliographie). En tout cas, cette suite d'opérations propose, selon diverses formulations :

- un moyen prouvable de résoudre un problème,
- une intermédiation sociale irréfutable entre un problème et une solution,
- ou encore, permet de résoudre de façon non-réfutable des problèmes communs.

Forcément, l'algorithme standardise et simplifie *(inconvénient)* mais à la vitesse électronique *(avantage)*. Toujours en apprentissage, il peut à tout instant produire une simulation «en information pure et parfaite, d'une situation réelle dont l'information est imparfaite et incomplète». Suivons cette étude des *Archives de la philosophie du droit* : «Les exceptions coûtent cher dans le code… La performance économique de la rente des MEAs *(Modèles Economiques Algorithmiques)* est directement dépendante des effets d'échelle et d'éventail que l'algorithme peut produire. C'est justement parce que ces MEAs peuvent s'absoudre des 'contextes' locaux, que leur avantage de coût absolu est si important.»

Décodeur : l'algorithme fonce dans le tas et rabote ce qui dépasse. Puisant sans cesse et à toute vitesse dans un flux immense et continu de corrélations associant des millions d'individus (grands nombres fournis par le *Big Data*), à des myriades de lieux, contacts, constantes et comportements, il élabore des modèles probabilistes affinés par apprentissage.

Exemple : pour une étude de consommation, l'algorithme créera et affinera (par voie statistique) des cibles commerciales, en calculant les traces qu'elles laissent sur Internet. D'où, disent les *Data Scientists*, sa capacité à *prédire* les comportements individuels tout comme les risques de sécurité. Aujourd'hui les algorithmes opèrent dans les domaines cruciaux de l'existence humaine : santé, amour, culture, finance, transports, etc. Ils dominent déjà :

- Le monde de la popularité (mesures d'audiences) ;
- Les classements de l'information (cybermméritocratie) ;
- Les mesures de réputation (réseaux sociaux, personnes et produits) ;
- Le domaine des prédictions comportementales (études de consommation).

Mais ces algorithmes ne tombent pas de la lune et ne surgissent pas par génération spontanée : ils ont des créateurs (informaticiens, *data scientists*) et des commanditaires (les titans de la «Silicon Valley» qui en usent massivement). Bien plutôt, ces algorithmes sont (pour le moment) l'arme absolue de ces derniers, leur permettant, si besoin, de manipuler, contrôler et intimider ceux qu'ils veulent marginaliser ou de détruire («*disruption*»). Ainsi, disent les critiques, un algorithme n'est guère qu'une opinion formalisée par codage, transformée en processus automatisé de décision - pas la vérité du Bon Dieu.

Aujourd'hui, des algorithmes choisissent parmi les candidats à un emploi ; évaluent nos capacités de crédit et les risques de récidive de détenus. Est-ce sans risque ? On a vu que ces outils numériques n'étaient jamais neutres - mais sont-ils loyaux ? Là encore de forts doutes existent. N'en exposons qu'un, avant d'entrer dans le vif du sujet.

Récemment (*New York Times International*, 3/08/2016, *bibliographie*) des défenseurs des libertés civiques ont saisi la Cour suprême du Wisconsin : un audit du logiciel évaluant les risques de récidive des détenus révélait des verdicts biaisés en défaveur des Noirs dans 40% des cas ; les Afro-Américains se voyant constamment affecter un taux de récidive future deux fois supérieur aux Blancs.

Ce logiciel n'aidait pas la justice, il créait de la discrimination. La Cour suprême du Wisconsin a donc tranché : désormais, un algorithme ne décidera plus seul d'une mise en liberté provisoire ou d'un maintien en prison. Et ce logiciel devra afficher clairement son taux d'erreur réel. Mais dans le monde magique de l'Internet, qui a cette prudence ? Pas grand monde, on va le voir.

Police et justice «prédictives», vraiment ?

Il existe, nous chantent (en 2015) des médias naïfs ou manipulés, des logiciels portant sur la «criminalité prédictive» ; d'ores et déjà en Europe (Allemagne, Suisse) ces logiciels servent «à déterminer les risques de délits, les lieux d'infractions, le mode opératoire et le professionnalisme des auteurs d'infractions». Le tout, en mode conte de fées - voire publicité rédactionnelle : «Et si l'on pouvait prédire où et quand auront lieu les prochains crimes et délits ? Cela ressemble à un scénario hollywoodien mais aux Etats-Unis, c'est déjà la réalité. Cela s'appelle la police prédictive. Des scientifiques, des entreprises, établissent les futures cartes de la délinquance en utilisant des algorithmes, des formules mathématiques… Certaines villes vont même plus loin et disent prédire, non pas où auront lieu les crimes, mais qui va les commettre». *(TV News - 29/12/2015, bibliographie)*.

Mieux ! Microsoft a développé un logiciel sachant «prédire le futur» et dire si un criminel récidivera dans les six mois. Il dit juste dans 91% des cas... Microsoft a beaucoup investi dans le développement des technologies prédictives. *(Business Insider, 17/12/2015, bibliographie)*

L'enthousiasme est contagieux : déjà, *Mediapart (20/05/2015, bibliographie)* a annoncé que le ministère français de l'intérieur se lance dans la police prédictive ; qu'il développe «un projet d'analyse et de prédiction de la criminalité», à partir d'une «démarche de renseignement criminel qui consiste, à partir d'une compréhension de la criminalité, à anticiper les phénomènes», tout cela, pour «prédire l'apparition des phénomènes criminels». Comment fonctionne ce «Predpol à la française» (*Big data* plus algorithmes prédictifs)? Le modèle est «basé sur les infractions constatées entre 2008 et 2013. S'il est validé et se vérifie sur les faits de 2014, nous le projetons sur l'année 2015».

Mais ces myopes journalistes et promoteurs du «Predpol à la française» ne semblent pas avoir repéré que la plupart des articles sur les technologies prédictives émanent d'une unique boîte de com' nommée «*Fusion*». Lisez les articles vantant la «police prédictive» : on y trouve des phrases comme «*according to a video discovered by Fusion*». Voyons ce que cette société américaine nous dit d'elle même (dans sa langue). Fusion produit du «*high impact digital advertising*» ; elle sait placer ses contenus «*within the heart of editorial content*»... «*We tell the most impactful stories... we create the most impactful conversations*» ajoute-t-elle, fière de rouler des journalistes trop pressés, se ruant sur des sujets tout prêts - et gratuits - sans s'étonner plus que cela du cadeau.

Avis à ces journalistes : qu'ils visitent le site de *Fusion* «*The media brand for a young, diverse and inclusive world*» ils y découvriront les habits neufs de la bonne vieille pub' rédactionnelle.

Après les miroirs aux alouettes médiatiques, le fond de l'affaire. En soulignant d'abord que l'idée de filtrer par voie de modélisation des millions de données sur de bénignes incivilités, permette de prévenir des crimes graves est, à ce jour, hautement hypothétique.

Voyons ce que disent de vrais experts ès-informatique. Ils sont moins fascinés que ces journalistes et politiciens qui, vivant trop souvent en symbiose, se contaminent les uns les autres. Ces experts observent que les logiciels de prédiction criminelle ne font qu'agréger et analyser des faits criminels passés puis calculent, heure par heure et géographiquement, où les crimes «doivent» se commettre ; ils les traduisent alors en «points chauds» (*hotspots*) sur la carte. Comme d'usage, Predpol & co. «prédisent» l'avenir à partir du passé.

Maintenant, souvenons-nous de ce nous avons dit du codage d'ersatz, faute de données pertinentes : si l'on code les seuls

crimes sérieux dans un logiciel Predpol ou analogue, on manque de grain à moudre, l'échantillon est trop réduit - donc peu ou pas de *hotspots* sur la carte. Il faut alors y inclure des délits, actes asociaux ou incivilités, selon une lecture biaisée de la fameuse théorie du «carreau cassé» de James Q. Wilson - en réalité bien plus subtile.

Selon cette simplette lecture, réprimer les délits permet de prévenir les crimes. Mais en fait, la standardisation étouffe statistiquement le logiciel : en principe créé pour cibler les crimes, il finit par ne «voir» que les incivilités.

Seconde critique : le côté bonneteau, «à tous les coups on gagne» ou prédiction auto-réalisatrice de Predpol & co :

- Predpol signale un *hotspot*, un policier s'y rend. Une infraction s'y commet, Predpol a raison. Pas d'infraction : Predpol a raison aussi, car le déplacement du policier l'a empêchée.

- Predpol signale un *hotspot* mais nul policier ne se rend sur les lieux : Ce policier apprend alors qu'une infraction s'y est commise : Predpol avait raison ! Rien n'arrive, rien n'est enregistré - Predpol n'avait pas tort.

Essai de Predpol à Oakland (Cal.) ville à majorité Noire. Les *hotspots* sont tous dans des quartiers noirs où les policiers passaient déjà leur temps. Predpol valide bêtement ce que la police fait déjà - mais «oublie» les quartiers blancs de la ville, où se consomme pourtant plus de drogue qu'ailleurs.

A Los Angeles, (2e force de police du pays, après New York City), quand les policiers arpentent les *hotspots* où ils allaient déjà avant, ceux-ci deviennent *encore* plus «chauds» ! (Prophétie auto-réalisatrice).

Troisième critique : Predpol réinvente l'eau chaude, prédit des banalités. Car tout policier sait que dans la criminalité des rues, le «gibier» s'adapte : quand la police multiplie les descentes dans un quartier ou sur un *hotspot*, le comportement des habitants et des criminels évolue. Or avant Predpol, les policiers n'agissaient pas au doigt mouillé. Et le fait d'être dirigés par des algorithmes les déresponsabilise, les démoralise. Comme ricane un cadre de la police de Burbank (Cal.) «Allez signaler à un gars qui pêche depuis vingt ans où il y a du poisson…».

Mêmes doutes sur la justice prédictive : les craintes s'accumulent sur la force normative de l'algorithme. Car si la justice d'un Etat de droit jauge la gravité du crime et les remords du malfaiteur ; le logiciel, lui, n'intègre *que* les données biographiques *passées* de celui dont il évalue le risque.

Quel destin pour un détenu à qui un logiciel «prédisant» la récidive (*automated risk assessment tool*), et non un juge, rejette la demande de libération conditionnelle ? Ne verra-t-il pas ses demandes sans cesse rejetées, hors de toute étude de son parcours

personnel ? Pire, la machine ne prendra-t-elle pas ce détenu comme variable d'ajustement de la population incarcérée ?

«Prédictif» : qu'est ce qui «marche» aujourd'hui ?

Les logiciels de type Predpol, pas trop : Richmond (Cal.) n'a pas renouvelé son contrat de trois ans, car la municipalité n'y voyait pas de baisse réelle des crimes sérieux. Burbank ne l'utilise plus car, disent les policiers locaux, ils n'ont pas besoin qu'un logiciel leur apprenne ce qu'ils savent déjà. Donc en Californie (où tout a commencé) le doute s'installe.

Les logiciels d'analyse des comportements anormaux («*Behavioral Recognition Systems*») semblent plus fiables car ici, considérer les précédents est pertinent. Un individu tourne autour d'un bâtiment et tente d'ouvrir les issues de secours... Dans une gare, un ivrogne titube trop près des rails... Des logiciels pré-curseurs peuvent «comprendre» de telles situations et ainsi, prévenir des intrusions ou des chutes sur la voie ferrée.

Voyons maintenant ces systèmes face à la menace terroriste. A ce jour, l'échec y est total. Depuis vingt ans, Washington dépense des fortunes à imaginer des «*watch lists*» efficaces de terroristes - pas de *futurs* terroristes, mais d'individus *déjà* actifs. Mais quels sont les symptômes d'un basculement dans la terreur ? Nul n'en sait rien - ni même d'abord, si ces symptômes existent. Or, quand gérer le présent est déjà si ardu, comment capter le futur ? Ce que la phénoménologie, discipline philosophique férue de temporalité, nomme le «domaine du possible» ?

Concrètement : comment repérer *à temps* Larossi Abballa[6] parmi dix mille «radicalisés» ? Aujourd'hui encore, le Renseignement intérieur français n'a pas grande compétence en matière d'anticipation (décèlement précoce). Certes Abballa multipliait les courriels inquiétants (*J'ai soif de sang... Dieu m'est témoin... Anéantissons les infidèles*) mais maints fanatiques disent de même, et parmi eux, sans doute y en a-t-il autant que de tels propos défoulent, que d'autres que cela excite.

A ce jour, le modèle antiterroriste prédictif est bel et bien hors de portée. Nul logiciel n'existe, qui permette de retrouver l'aiguille terroriste dans la meule de foin des radicalisés. De même, dans un domaine proche, n'a-t-on jamais pu concevoir un efficace système numérisé de prévention des suicides.

Pour conclure, élargissons notre propos. La prédiction stratégique est toujours fort difficile. Récemment, voici le «Brexit», que tous les bourgeois progressistes, tous les bobos libertaires d'Europe et alentours, qualifiaient de «crime». A la clôture du vote, 84% des parieurs des sites de jeux en ligne britanniques voyaient vaincre le «Remain».

Le «Brexit» a assommé la City de Londres, les politiciens et médias (désormais comme en France, un symbiotique hybride), plus les services spéciaux américains, fétichistes du *high-tech*. Lugubre, une agence de presse lamentait sa «difficulté à prévoir de tels chocs, même avec l'aide d'outils comme des algorithmes conçus pour sentir 'vibrer' média sociaux» *(Reuters, 25/06/2016, bibliographie*). Même les algorithmes n'y ont rien pu ! A qui se fier. Ce sera notre conclusion.

Sources de l'étude

• *Ouvrages (ordre alphabétique)*

Conway Flo & Siegelman Jim «Dark hero of the information age: in search of Robert Wiener», Basic Books, US, 2005

Goldsmith Jack & Wu Tim, «Who controls the Internet ? Illusions of a borderless world», Oxford University Press, London, 2006

Goodman Marc «Future crimes», Corgi Books - Penguin-Random, US, 2015

Malcomson Scott «Splinternet - how geopolitics and commerce are fragmenting the World Wide Web», OR Books, US, 2016

O'Neil Cathy «Weapons of math destruction», Allen Lane - Penguin Books, UK, 2016

Turner Fred «From counterculture to cyberculture», University of Chicago Press, US, 2008

Valéry Paul «Regards sur le monde actuel», Folio-Essais, 1994

Wiener Norbert «Cybernetics, or control and communication in the animal and the machine» Wiley, US, 1948

• *Médias, etc. (ordre généalogique)*

L'Expansion - 16/10/2016 «Big data, algorithmes : l'esprit porté par Silicon Valley est totalitaire»

Business Insider - 10/10/2016 «Crime prediction tool may be reinforcing discriminatory policy»

Le Parisien - 12/08/2016 (police prédictive) «Un usage de plus en plus répandu»

Michael Brenner (Blog) - 5/08/2016 «Silicon Valley: inferno / purgatorio / paradiso»

New York Times International - 3/08/2016 «Make algorithms accountable»

Reuters - 25/06/2016 «Brexit baffled punters, pundits and fund managers to the very end»

New York Times International - 22/06/2016 «Identifying future killers out of a sea of suspects»

New York Times International - 28/03/2016 «Studies fail to pinpoint who turns to terrorism»

TV News - 29/12/2015 «Les devins du crime aux Etats-Unis : reportage dans *Envoyé Spécial*»

Business Insider - 17/12/2015 «Microsoft is building an app that can predict criminal behavior»

Tech Insider - 15/12/2015 «Computer algorithms are now deciding wether prisoners get parole»

Libération - 10/10/2015 «En calculant nos traces, les algorithmes reproduisent les inégalités entre les individus»

Tech Insider - 19/08/2015 «Artificially intelligent security cameras are spotting crime before they happen»

New York Times International - 3/08/2016 «When algorithms are guilty of human biases»

Le Monde (Blogs) 27/06/2015 (Internet-Actu) «Police prédictive : la prédiction des banalités»

Mediapart - 25/05/2015 «Gendarmes et industriels imaginent un nouveau logiciel pour prédire le crime» *(même jour)* «L'algorithme n'est pas un système de prédiction mais d'intervention»

Institut Diderot, printemps 2015 «L'avenir des Big data»

Archives de philosophie du droit - (58) 2015 «L'algorithme et l'ordre public»

Science - 04/2014 - «The parable of Google flu: traps in the Big data analysis»

Esquire - 10/1971 «The secrets of the little blue box»

Notes

[1] Martin Heidegger & Eugen Fink «Héraclite, séminaire du semestre d'hiver 1966-1967», NRF Gallimard, 1973.
[2] Cf. Marc Goodman, fondateur du *Future crimes Institute* et professeur à la *Singularity University*, voir bibliographie.
[3] Auto-absolution américaine d'usage baptisée *colorful past*.
[4] Entre la *Grand Fleet* britannique et la *Hochseeflotte* allemande, 31 mai-1er juin 1916, 250 navires engagés ; 14 navires britanniques coulés, 11 allemands ; des milliers de morts ; pas de vainqueur décisif.
[5] Norbert Wiener «I am a mathematician», MIT Press, 1953.
[6] En juin 2016, il poignarde à mort, dans leur pavillon de Magnanville (Yvelines), deux policiers français sans liens directs avec l'antiterrorisme, puis est abattu par des forces d'intervention.

BULLETIN D'ABONNEMENT OU DE RÉABONNEMENT

Sécurité Globale

Bulletin d'abonnement ou de réabonnement

À retourner accompagné de votre règlement aux
Éditions ESKA – 12, rue du Quatre-Septembre, 75002 PARIS
Tél. : 01 42 86 55 65 – Fax : 01 42 60 45 35

http://www.eska.fr

M, Mme, Mlle _____ Prénom _____

Société/Institution _____

N° _____ Rue _____

Code postal _____ Ville _____

Pays _____

Adresse électronique _____

TARIFS D'ABONNEMENTS*

	France particulier	France société/ institution	Etranger particulier	Etranger société/ institution
1 an (2017)	❑ 109 €	❑ 138 €	❑ 133 €	❑ 164 €
2 ans (2017 et 2018)	❑ 196 €	❑ 245 €	❑ 235 €	❑ 293 €

* Abonnements souscrits à l'année civile (janvier à décembre).

❑ Je souscris un abonnement pour ❑ 1 an ❑ 2 ans

Je joins mon règlement de _____ Euros

❑ par chèque bancaire à l'ordre des Éditions ESKA

❑ par virement bancaire aux Éditions ESKA – BNP Paris Champs Elysées 30004/00804/ compte : 00010139858 36

❑ par carte bancaire : merci d'indiquer votre numéro de compte et la date d'expiration
N° carte bancaire : ❑ Visa ❑ Eurocard/Mastercard

|_|_|_|_| |_|_|_|_| |_|_|_|_| |_|_|_|_|

Date d'expiration : |_|_|_|_| Signature :

Derniers numéros parus

Sécurité globale 7 | 2016 (nouvelle série) : Islam activiste, réaction et révolution
Sécurité globale 6 | 2016 (nouvelle série) : Le monde criminel à l'horizon 2025
Sécurité globale 5 | 2016 (nouvelle série) : Dossier Stupéfiants
Sécurité globale 3-4 | 2015 (nouvelle série) : Toujours plus cyber-menacées : les collectivités territoriales / « Police prédictive » : les belles histoires de l'Oncle Predpol
Sécurité globale 2 | 2015 (nouvelle série) : Bandes, Braquages, Terreur
Sécurité globale 1 | 2015 (nouvelle série) : Iran 2015 : Qui gouverne à Téhéran (et comment) ?
Sécurité globale 25-26 | 2013 : La France face à ses ESSD
Sécurité globale 24 | 2013 : Cyber : la guerre a commencé (2e partie)
Sécurité globale 23 | 2013 : Cyber : la guerre a commencé (1re partie)
Sécurité globale 22 | 2012 : La Suisse : nation militaire
Sécurité globale 21 | 2012 : L'eau, enjeu de sécurité et de développement

ÉDITIONS ESKA
12 rue du Quatre-Septembre - 75002 Paris, France
Tél. : 01 42 86 55 65 | Fax : 01 42 60 45 35
http://www.eska.fr