Benoît Dupont

Cybercriminalité

Approche écosystémique de l'espace numérique

ARMAND COLIN

Illustration de couverture : © grafxart – Shutterstock.

Mise en page : Nord Compo

Sauf mention contraire, les figures ont été réalisées par l'auteur

NOUS NOUS ENGAGEONS EN FAVEUR DE L'ENVIRONNEMENT :

Nos livres sont imprimés sur des papiers certifiés pour réduire notre impact sur l'environnement.

Le format de nos ouvrages est pensé afin d'optimiser l'utilisation du papier.

Depuis plus de 30 ans, nous imprimons 70 % de nos livres en France et 25 % en Europe et nous mettons tout en œuvre pour augmenter cet engagement auprès des imprimeurs français.

Nous limitons l'utilisation du plastique sur nos ouvrages (film sur les couvertures et les livres).

Armand Colin est une marque de Dunod Éditeur,
11 rue Paul Bert, 92240 Malakoff

ISBN 978-2-200-63796-5

Remerciements

La gestation de cet ouvrage aura duré une demi-douzaine d'années, soit bien plus longtemps que je ne l'avais imaginé quand j'en ai esquissé les premières lignes et que je pensais de manière insouciante en avoir terminé en quelques mois. Durant toutes ces années, j'ai eu le privilège de partager, de valider ou de remanier les idées qui traversent cet ouvrage avec un nombre considérable de collègues, d'étudiants et de professionnels qui ont fait preuve d'une patience et d'une générosité infinies. Ma dette envers eux est immense et leur liste est trop longue pour que je puisse ici tous les nommer.

Je dois toutefois exprimer une gratitude toute spéciale à Jean-Paul Brodeur et à Carlo Morselli, dont l'invitation permanente à remettre en question le statu quo et à ne pas fuir les sujets controversés reste une source d'inspiration quotidienne, malgré leur disparition prématurée. Je remercie également Peter Grabosky, qui m'a fait comprendre il y a un quart de siècle que le futur de la criminologie passerait par sa capacité à incorporer la cybercriminalité aux questions de recherche et aux cadres analytiques existant, et que l'innovation en matière de régulation et de gouvernance pouvait être sans limites. Nos conversations se sont éternisées depuis autour d'un cassoulet fumant ou d'une soupe à la queue de kangourou. Clifford Shearing, à travers nos discussions infusées de son intelligence pétillante, m'a permis de mieux prendre conscience de l'évolution des rationalités et des pratiques de gestion des risques, et de la dilution des barrières traditionnelles entre nature, humains et machines. Son goût pour la pâte feuilletée m'a aussi permis de savourer des croissants de compétition dans les endroits les plus improbables.

Je tiens aussi à remercier ces chercheuses et chercheurs qui ont fait de la cybercriminalité leur principal champ d'étude, et qui se sont toujours montrés disposés à débattre et à partager leur point de vue et leurs données, dans un souci de collégialité qui les honore et qui nous permet de construire un savoir empirique défiant les clichés et les stéréotypes. Je pense en particulier à Maria Bada, Bilel Benbouzid, David Décary-Hétu, Francis Fortin, Tom Holt, Alice Hutchings, Rutger Leukfeldt, Jonathan Lusthaus, Mike Levi, David Maimon, Masarah Paquet-Clouston, Quentin Rossy, Samuel Tanner, Daniel Ventre, ou encore Chad Whelan. Bien que travaillant sur d'autres sujets de recherche, Frédéric Ocqueteau n'a jamais été avare de son érudition sociologique et m'a incité à examiner les continuités liant le monde incarné et le monde numérique, plutôt que de me focaliser uniquement sur les ruptures.

J'ai eu le plaisir de présenter certains chapitres de ce livre dans le cadre de séminaires de recherche ou de conférences académiques, notamment à l'Université d'Oxford, à l'Université d'État du Michigan, à l'Université

de Lausanne, à l'Université de Bruxelles, à l'Université Sungkyunkwan, à l'Institut coréen de criminologie et de justice (KICJ), à l'Université de Sydney, à l'Université de Nouvelle-Galles-du-Sud, à l'Université Deakin, au Centre de recherches sociologiques sur le droit et les institutions pénales (CESDIP), aux conférences annuelles de la Société américaine de criminologie, aux ateliers Human Factor in Cybercrime, et aux rencontres de l'Association internationale des criminologues de langue française. Chacune de ces présentations et les riches échanges auxquels elles ont donné lieu m'ont permis d'affiner des idées parfois encore à l'état embryonnaire, et m'ont prémuni d'une tentation simplificatrice grâce aux objections et suggestions bienveillantes de mes très chers collègues.

La plus grande part de cet ouvrage a été rédigée en mode nomade, dans un périple qui m'a mené de l'Asie aux Antilles. Cette aventure n'aurait pas été aussi productive sans l'aide précieuse du très résilient et spirituel Hyun-Wook Chun à Séoul, et l'accueil chaleureux de Yannick Louis-Hodebar, Patrick Desjardins et Josselin Troupé à Pointe-à-Pitre.

Je n'aurais jamais eu le loisir de participer à toutes ces activités scientifiques et de me consacrer exclusivement à cet ouvrage pendant de longs mois si à Montréal, Fyscillia Ream et Michael Joyce n'avaient vaillamment tenu le fort, respectivement à la coordination scientifique de la Chaire de recherche en Prévention de la cybercriminalité et à la direction exécutive du Human-Centric Cybersecurity Partnership. Je les remercie de tout cœur et j'espère pouvoir leur rendre la pareille dans un avenir pas si lointain.

Chez Armand Colin, Julie Beny a immédiatement réservé un accueil enthousiaste à ce manuscrit, et son expérience éditoriale a permis d'en alléger le style et de le rendre plus accessible à un lectorat de non-initiés. Les erreurs qui pourraient subsister restent ma seule responsabilité.

Enfin, j'ai une pensée particulière pour Virginie, dont la curiosité, l'énergie, l'enthousiasme et l'humour me nourrissent chaque jour, et qui a toléré au cours de cette année de nomadisme sabbatique mes défections académiques. Et bien entendu pour ma fille Maxime, dont la gouaille et l'amour inconditionnel me ravissent.

Introduction

Quel est le point commun entre une ingénieure informatique de la Silicon Valley en train de développer une technologie de rupture, un entrepreneur russe cherchant à étendre ses activités à l'international, un Youtubeur français revendiquant 500 000 abonnés, et la victime canadienne d'une fraude amoureuse ? Tous font partie, sans en avoir forcément conscience, de l'écosystème du cybercrime.

L'ingénieure informatique développe de nouveaux produits et services pour son employeur dans un contexte économique de compétition féroce où on lui demande d'innover en permanence et de lancer, sur un rythme toujours plus effréné, de nouveaux produits qui sauront capturer des parts de marchés assurant à l'entreprise une croissance soutenue. Cette injonction frénétique à l'innovation la pousse à négliger d'autres aspects pourtant essentiels de son travail comme la sécurité des produits qu'elle conçoit. Les cyberdélinquants exploitent avidement cette manne de failles aisément évitables. L'entrepreneur russe est l'un d'entre eux. Son modèle d'affaire repose sur l'accès à une riche expertise technique disponible dans les pays de l'ancien bloc soviétique et sur une quasi-impunité de la part des services de sécurité de son pays d'origine. Ces derniers le laissent opérer en paix, tant qu'il évite de cibler des victimes locales et qu'il collabore ponctuellement lorsqu'on lui en fait la demande. Immergé au cœur d'un vaste réseau de coopération criminelle dont les ramifications se déploient à l'échelle internationale, notre entrepreneur criminel doit maintenir une posture de vigilance constante, afin d'échapper à la surveillance et aux activités répressives ou perturbatrices d'un vaste éventail d'organisations de sécurité. Bien que l'on pense spontanément à des organisations policières ou à des entreprises spécialisées en cybersécurité lorsqu'on évoque les capacités de réponse aux problèmes de cybercriminalité, notre Youtubeur français appartient lui aussi à cette communauté d'acteurs institutionnels et individuels tentant de freiner la croissance exponentielle de la cybercriminalité. Ses vidéos, diffusées une à deux fois par semaine expliquent dans un langage accessible à tous les rouages internes des fraudes en ligne les plus répandues. Il n'hésite pas à tendre des pièges à des cyberdélinquants peu attentifs en se faisant passer pour une victime vulnérable, produisant un spectacle vengeur censé rétablir une certaine justice au nom des millions de victimes frappées par la prolifération de la cybercriminalité. Notre victime canadienne est l'une de ces millions de personnes tombées dans les filets des cyberdélinquants. Souvent caricaturée dans les médias comme excessivement naïve ou cupide, elle n'a fait que succomber à des stratégies de manipulation psychologique sophistiquées. Ses besoins ne sont pas réellement pris en compte par les organisations policières,

vers lesquelles elle hésite à se tourner par crainte d'être traitée avec condescendance. C'est donc en ligne, sur des forums d'entraide mutuelle animés par d'autres victimes, qu'elle trouve le soutien psychologique et les informations sur les démarches à entreprendre pour tenter de récupérer l'argent perdu.

Ces quatre protagonistes, dont les profils fictifs ont été dressés à l'aide d'éléments composites empruntés à des personnes existantes, ne constituent qu'un minuscule échantillon de l'immense diversité des entités qui peuplent le vaste écosystème du cybercrime. S'ils ont peu de chances de s'être déjà rencontrés, ils sont toutefois irrémédiablement liés les uns aux autres par des chaînes d'interdépendances qui découlent de leurs décisions individuelles, de leurs préférences, et de leurs capacités d'action. Qu'ils soient engagés dans des relations de compétition, de prédation ou de collaboration, les effets cumulatifs de ces interactions ne sont que très rarement analysés dans leur globalité, alors qu'ils structurent la cybercriminalité contemporaine et en influencent l'évolution. Cet état de fait est en grande partie attribuable aux logiques disciplinaires réductionnistes qui dominent encore les recherches sur la cybercriminalité.

Alors que les criminologues s'intéressent principalement au profil et aux motivations des cyberdélinquants, et plus rarement aux scripts criminels qui leurs permettent de convertir des vulnérabilités techniques ou humaines en profits illicites, les informaticiens examinent les propriétés du code malveillant déployé par les pirates informatiques ou les sources de défaillances techniques facilitant l'exploitation de ce code. Les juristes examinent, quant à eux, les problèmes de qualification des comportements problématiques en ligne et les dispositifs légaux qui permettraient d'en harmoniser la prise en charge à l'échelle internationale. Les psychologues privilégient l'étude des traits de personnalité qui pourraient permettre de prédire la susceptibilité de certaines personnes à succomber aux offres douteuses de parfaits inconnus en ligne. Les politologues sont pour leur part préoccupés par le recoupement entre les activités criminelles de certains groupes de pirates informatiques et l'instrumentalisation de ces groupes par des États voyous qui s'en servent comme de véritables corsaires numériques. Plus de quarante autres disciplines traitent, sous des angles variés, ces notions de cybercriminalité et de cybersécurité, allant de la philosophie à l'économie, en passant par les arts ou encore la santé publique (Carley, 2020).

Leurs approches restent pourtant artificiellement segmentées, prisonnières de cadres théoriques et de méthodologies empiriques étriquées, dans des communautés épistémiques de plus en plus spécialisées. La complémentarité et les arrimages indispensables à l'émergence d'une interdisciplinarité émancipatrice peinent à se matérialiser, en dépit d'un large consensus sur les limites de la myopie disciplinaire actuelle pour répondre à la complexité des défis environnementaux, technologiques et sociétaux auxquels l'humanité se trouve confrontée (Braithwaite, 2014).

Revendiquant l'urgence de transgresser un cloisonnement disciplinaire, cet ouvrage propose donc une approche intégratrice de la cybercriminalité qui s'inspire de la démarche scientifique et des concepts forgés par l'écologie, cette science des relations. Il ne s'agit pas de transposer littéralement des règles immuables découvertes dans le monde végétal ou animal à des relations

humaines qui obéissent à leurs propres dynamiques, assez souvent imprévisibles, mais d'emprunter plutôt à l'écologie ses cadres d'analyse ancrés dans la complexité d'une nature aux équilibres précaires et en perpétuel changement, sa préoccupation constante pour l'examen approfondi des interactions et de l'environnement au sein duquel elles se déploient, son intérêt pour les effets émergents qui découlent des vastes réseaux d'interdépendances liant ensemble des centaines d'espèces, et sa capacité à penser les adaptations réciproques qui en résultent.

Cette écologie du cybercrime n'est pas uniquement d'ordre métaphorique. Elle s'approprie les méthodes qui aident à catégoriser les entités étudiées en populations et en communautés (industrielle, délinquante, et de la sécurité), les types d'interactions qui structurent ces communautés (coopération, compétition, prédation), ou encore les stratégies d'adaptation qui caractérisent leur coévolution (camouflage, mimétisme, évitement, mouvement, etc.). Recourir à la perspective écologique nous permet ainsi de mieux percevoir les limites d'une approche réductionniste – encore dominante – qui tente de comprendre la cybercriminalité sans se pencher de manière approfondie sur le fonctionnement des industries qui produisent les biens et les services à l'origine de la révolution numérique et en gèrent les infrastructures techniques. Ce réductionnisme omet fréquemment d'examiner les avantages compétitifs que les réseaux criminels tirent des technologies numériques pour surmonter les défis organisationnels auxquels ils sont confrontés dans un environnement hostile, ou encore ignore les mécanismes de contrôle et les modalités d'intervention institutionnelle permettant de prévenir ou de réduire les risques inhérents à la transformation numérique de la société. La perspective écologique met ainsi à notre disposition un riche répertoire d'outils permettant de dévoiler l'entrelacement complexe d'interactions entre acteurs licites et illicites qui conduisent à la prolifération des cybercrimes observée depuis un quart de siècle, mais aussi à la mise en place de réponses institutionnelles aux modalités aussi variées que prometteuses.

L'écologie du cybercrime ébauchée dans ces pages ne renie pas pour autant les apports considérables des nombreux auteurs issus des sciences sociales qui ont fait progresser notre compréhension des transformations induites par la mondialisation des échanges et la technicisation des activités humaines. Elle s'enracine bien au contraire dans les contributions magistrales de trois penseurs qui nous aident à appréhender la complexité du monde contemporain et nous invitent à nous extirper du confort des cadres établis. Norbert Elias et son concept de configuration nous permet de dépasser la dichotomie classique entre individu et société pour examiner sans *a priori* comment les liens d'interdépendance, qu'ils soient de coopération ou de conflit, entre individus et groupes sociaux produisent par un processus d'accumulation et d'imbrication spécifique à chaque contexte de nouveaux assemblages aux équilibres changeants. Manuel Castells a, quant à lui, démontré comment le réseau comme structure sociale et organisationnelle permet de comprendre l'accélération de la mondialisation des échanges et certaines dynamiques émergentes de concentration du pouvoir et de la richesse. Les flux de données, de connaissance, et de confiance qui donnent vie à ces réseaux dessinent une morphologie

sociale optimisée, accélérée et amplifiée par des technologies numériques dont les effets perturbateurs sont parfois sous-estimés par les chercheurs et les décideurs politiques, mais avidement exploités par les entrepreneurs et les délinquants. Finalement, l'œuvre de Bruno Latour nous incite à prendre au sérieux les changements provoqués par les technologies en cessant de ségréguer ces dernières des catégories sociales existantes pour en faire des actrices à part entière de la société. Les assemblages humains-machines qui en découlent peuvent alors être étudiés de manière à révéler des configurations sociales inédites, mais non moins puissantes. Ces trois approches théoriques illustrent la compatibilité fondamentale de l'écologie du cybercrime avec des paradigmes sociologiques soucieux de penser la complexité dans un monde d'incertitudes et d'imprévisibilité, et leur complémentarité réciproque.

Bien qu'il tente de synthétiser de manière aussi accessible que possible une grande quantité de résultats de recherche organisés selon une perspective théorique d'inspiration écologique, cet ouvrage n'est pas réservé à une audience académique. Nous sommes tous confrontés dans notre usage quotidien des outils numériques à des manifestations de la cybercriminalité, que ce soit à travers des messages d'hameçonnage quotidiens, l'infection de nos équipements informatiques par des logiciels malveillants, ou des tentatives de fraude provenant des plateformes de petites annonces ou de rencontres en ligne. Pourtant, les représentations de ce phénomène par les médias grand public restent trop souvent caricaturales : des pirates informatiques malveillants au visage dissimulé dans l'ombre d'un sweat-shirt à capuche et capables de piller nos comptes bancaires et de réduire notre vie sociale en cendres en quelques lignes de code, des victimes trop naïves ou cupides qui contribuent par leur crédulité et leur impulsivité à leur propre déconvenue, des enquêteurs policiers indifférents, incompétents ou impuissants à retracer et arrêter des cybercriminels réfugiés dans des pays leur offrant l'impunité judiciaire, ou encore des ingénieurs en cybersécurité s'évertuant à inventer de nouvelles technologies protectrices que les utilisateurs ne cessent de saboter par leur comportement irresponsable (le fameux utilisateur comme « maillon faible » de la cybersécurité). Ces représentations reflètent la pauvreté de nos connaissances sur le sujet et la difficulté de communiquer l'ampleur du problème, sa complexité, mais aussi les solutions disponibles sur un registre accessible au plus grand nombre.

Enfin, sans prétendre détenir de solution miracle et universelle, j'essaierai néanmoins de montrer quelles sont les implications et applications pratiques de l'écologie du cybercrime sur les politiques publiques de prévention et de lutte contre les risques numériques criminels. En invitant les praticiens et décideurs publics à enrichir leur répertoire d'action pour profiter pleinement de la diversité qui caractérise l'écosystème numérique, je proposerai quelques pistes concrètes inspirées d'initiatives et d'expérimentations prometteuses. Si des opportunités existent, des risques bien réels de dilution du pouvoir de l'État et du bien commun peuvent aussi résulter de ces nouvelles modalités de régulation, qu'il convient d'examiner sans complaisance.

Cet ouvrage se divise en cinq grandes parties, que le lecteur pourra parcourir de manière séquentielle en suivant la visite guidée que je lui propose de l'écosystème cybercriminel, ou dans lesquelles il pourra piocher selon ses propres

besoins et intérêts. Dans la première partie, je dresserai l'inventaire des outils théoriques disponibles pour penser la complexité des risques numériques. Le premier chapitre examine les contributions des trois sociologies majeures et complémentaires de Norbert Elias, Manuel Castells et Bruno Latour. Celles-ci offrent de précieuses clés de décryptage de la complexité du monde contemporain, et en particulier des transformations sociales induites par l'omniprésence des technologies numériques. Dans le chapitre 2, je propose d'ajouter l'écologie à la boîte à outils conceptuelle déjà bien garnie décrite au chapitre précédent. Cette science, d'abord utilisée pour analyser de manière systématique les interactions entre les espèces végétales et animales et leur environnement naturel, a rapidement été adoptée et adaptée par les sciences sociales qui ont tenté d'appliquer certaines de ses méthodes à l'étude de l'organisation des relations humaines. J'en proposerai une application qui aidera à saisir la complexité de l'écologie sans succomber aux chimères d'une scientificité illusoire.

La deuxième partie est consacrée à la présentation systématique des éléments de l'écosystème du cybercrime et de son contexte industriel. Dans le chapitre 3, les concepts de haut niveau empruntés à l'écologie sont transposés au contexte numérique. L'écosystème numérique et ses caractéristiques environnementales sont décrits, les trois communautés d'entités (industrielle, criminelle et de la sécurité) qui jouent un rôle important dans l'écosystème du cybercrime sont présentées, leurs modes d'interaction (compétition, prédation, coopération) intra- et interspécifiques sont énumérés, et les effets émergents auxquels la somme de ces interactions donnent lieu sont également discutés. Le chapitre 4 met ces concepts en application afin de montrer comment la communauté industrielle et la compétition extrême qui caractérise les interactions entre les entités qui la composent constituent un terreau particulièrement fertile à l'apparition de vulnérabilités exploitables par les cyberdélinquants. En d'autres termes, la prééminence d'une compétition perçue comme une menace existentielle à la survie des entreprises qui appartiennent à la communauté industrielle conduit ces dernières à négliger les mesures de sécurité qu'elles pourraient intégrer à leurs produits et services. Cela contribue à l'émergence d'un régime d'insécurité chronique pour les utilisateurs, qui est habilement et intensément exploité par les cyberdélinquants.

La troisième partie explore en détail le fonctionnement de la communauté criminelle, en commençant par examiner au chapitre 5 comment la délinquance traditionnelle intègre les outils numériques à ses pratiques afin d'en améliorer l'efficacité et d'en diminuer les risques. En prenant les exemples de la prostitution, du trafic de drogues, et de la consommation de pornographie juvénile, j'illustre comment les technologies numériques accélèrent l'innovation criminelle et comment la communauté délinquante s'approprie des outils initialement conçus pour d'autres utilisations, en examinant quelles fonctions sont particulièrement renforcées par ces usages. Le chapitre 6 délaisse la catégorie des crimes cyber-facilités pour plonger dans l'univers des crimes cyber-dépendants, où la technologie constitue la cible des activités criminelles et qui inclut de nouvelles formes de délinquance comme le piratage informatique. L'expertise technique requise pour mener ce type de crimes exige une division du travail qui façonne un mode d'organisation par projet assez novateur

et directement inspiré du fonctionnement des équipes décentralisées de la communauté industrielle. Si les outils numériques confèrent aux cybercriminels un net avantage concurrentiel pour mener leurs activités prédatrices, ils ne sont pas dénués d'inconvénients. Ils contribuent notamment à accentuer le dilemme de la confiance entre des individus qui ne se connaissent que par écrans interposés, et qui peuvent donc se trahir ou faire défection en toute impunité sans crainte de représailles. La nature éphémère des liens de co-délinquance qui est accentuée par les outils numériques donne ainsi lieu à diverses stratégies de renforcement de la confiance inspirées des plateformes numériques légales, dont l'efficacité reste cependant très fragile et sujette à manipulation. Le chapitre 7 vise à comprendre comment la communauté criminelle s'adapte afin de pouvoir continuer à générer des profits criminels dans un environnement hostile. Trois formes de coévolution sont à l'œuvre : une coévolution opportuniste, qui améliore l'efficience de la communauté criminelle par un parasitisme de la communauté de la sécurité, une coévolution défensive, qui parfait les chances de survie de la première en la soustrayant aux mesures de surveillance et de détection de la seconde, et finalement une coévolution stratégique, permettant l'amélioration de la performance criminelle dans un environnement fluctuant.

La quatrième partie se penche sur le fonctionnement de la communauté de la sécurité. Le chapitre 8 analyse les multiples causes à l'origine de la mésadaptation des institutions policières et judiciaires dans leurs réponses au problème maintenant bien connu de la cybercriminalité. Le manque de statistiques fiables, le déficit d'expertise interne, la réticence au recours à des compétences externes, l'accessibilité de la cryptographie aux cyberdélinquants, ou encore la rigidité de la culture organisationnelle expliquent pourquoi si peu d'enquêtes policières aboutissent à des arrestations et à des condamnations pénales par des tribunaux qui sont eux-mêmes bien mal équipés pour faire face à ce type d'affaires. Le chapitre 9 élargit le cadre d'analyse en soulignant le pluralisme de la communauté de la sécurité, qui incorpore bien d'autres capacités techniques et institutionnelles, dont la contribution à la prévention et au contrôle de la cybercriminalité est fréquemment sous-estimée. Une cartographie systématique des ressources pouvant être mobilisées offre alors une image moins déprimante des options d'intervention disponibles, par contraste avec le chapitre précédent.

La cinquième et dernière partie adopte une approche plus normative, afin de tirer les leçons des résultats présentés dans les chapitres précédents sur le fonctionnement et les interactions des trois communautés de l'écosystème et d'identifier les options de gouvernance et de régulation disponibles, ainsi que celles s'avérant prometteuses en termes d'efficacité. Le chapitre 10 présente une théorie de la régulation de la cybercriminalité qui s'appuie sur l'organisation en réseau des entités chargées de la répression et de la prévention, et sur la diversité des sources, des moteurs et de l'intensité de la régulation activées par ce réseau. Le chapitre 11 synthétise les contributions qu'une étude écologique de la cybercriminalité peut apporter aux sciences sociales, qu'il s'agisse de se doter d'outils permettant de mettre à jour des configurations inédites et imprévisibles, ou encore de dévoiler des rationalités concurrentes de cybersécurité qui nuisent parfois à la cohérence des interventions de l'État.

Finalement, l'écologie du cybercrime peut aussi inspirer la mise en œuvre de politiques publiques multilatérales de prévention et de lutte contre la cybercriminalité qui associent de près une grande diversité d'entités publiques et privées dans le souci du bien commun. Mais il est essentiel que ces politiques n'omettent pas de prendre en compte les défis démocratiques que représentent leur interprétabilité pour l'usager lambda, l'évaluation de leur efficacité réelle face à des promesses parfois irréalistes, leur imputabilité pour éviter les dérives d'une surveillance de masse ou d'une capture par des intérêts privés, et la résilience numérique renforcée pour tous les utilisateurs, y compris les plus vulnérables. À ces conditions seulement, peut-on espérer que l'écosystème du cybercrime atteigne un nouveau point d'équilibre où les activités prédatrices de la communauté criminelle seraient maintenues à des niveaux tolérables par une communauté industrielle mieux responsabilisée et une communauté de la sécurité dynamique et agile. Ce qui devrait permettre à la population de tirer pleinement profit des nombreux avantages de la technologie, sans avoir à vivre dans un état de nature numérique où la crainte de devenir une victime livrée à elle-même ferait de chaque interaction en ligne une source de risques à éviter plutôt qu'une opportunité émancipatrice.

Première partie

Penser la complexité des risques numériques

Chapitre 1

Sociologies de la complexité : nouvelles configurations société-humains-machines

La complexité inédite d'un monde dans lequel prolifèrent des flux mondialisés de personnes, de biens, de capitaux et de données qui remettent en question les structures politiques, sociales et juridiques établies constitue un défi analytique majeur pour les sciences sociales, plutôt habituées à étudier les groupes, les espaces ou les pratiques sociales de manière relativement circonscrite. Afin de nous aider à comprendre les nouveaux assemblages hybrides dont dépendent nos sociétés contemporaines et où s'enchevêtrent humains, machines et données, eux-mêmes structurés en une multitude d'institutions publiques, privées et communautaires, la sociologie met à notre disposition quelques cadres explicatifs unificateurs. Capables d'articuler de manière globale les systèmes d'interactions et d'interdépendances qui lient l'individuel et le collectif, le local et le mondial, ou encore l'humain et le technique, trois approches théoriques enracinées dans des traditions très diverses sont particulièrement adaptées à l'étude des risques induits par la révolution numérique.

Les configurations : dépasser l'opposition individu-société

Le concept de configuration a été élaboré par Norbert Elias avec comme objectif explicite la volonté d'apporter une réponse novatrice aux débats qui opposent les théories classiques de la société et de l'individu (Delmotte, 2010 : 31). Se revendiquant d'un « réalisme sociologique » (Elias et Dunning, 1986 : 272), cette approche préconise l'étude simultanée des deux niveaux d'observation inséparables que constituent l'individu et la société, et l'assouplissement des contraintes conceptuelles qui en font trop souvent des objets

de recherche antagonistes (Elias, 1991). Dans cette approche, les groupes d'individus, quelle que soit l'échelle à laquelle nous les étudions (de la cour royale à l'équipe de football ou au système international multipolaire), ne sont plus conçus comme des entités abstraites et cumulatives qui auraient une existence séparée de celle de leurs membres, mais sont au contraire identifiés comme des configurations, qu'Elias définit comme « ce type unique de structure qui résulte de la rencontre d'actions et d'expériences individuelles, de l'interdépendance fonctionnelle d'acteurs individuels dans les divers groupes auxquels ils appartiennent » (Elias, 1986 : 70). Réciproquement, les décisions et actions des individus, loin de s'avérer aussi autonomes qu'aiment à le penser les statisticiens, n'ont de sens que si on les interprète au prisme de ces mêmes relations d'interdépendance, qui en influencent les paramètres et la dynamique.

L'originalité du concept de configuration réside en grande partie dans son ambition de combler le gouffre qui sépare trop souvent les approches micro- et macrosociologiques, mais aussi dans sa plasticité, qui permet de l'appliquer à des types de processus sociaux extrêmement variés. C'est notamment à travers l'analyse de la société de cour ou de la dynamique de groupes sportifs (des équipes de football en l'occurrence) qu'Elias a pu illustrer l'application concrète de sa théorie (Elias, 1985 ; Elias et Dunning, 1986). La compatibilité de la sociologie configurationnelle avec des échelles d'analyse qui s'étendent d'un petit groupe d'individus (tels des joueurs de cartes réunis pour une partie entre amis) à des organisations complexes ou des nations entières la rend particulièrement adaptée à l'analyse des risques numériques, qui peuvent aussi bien être étudiés sous l'angle des groupes criminels qui s'adonnent au piratage informatique que sous celui des grandes entreprises qui en sont les cibles, ou des initiatives de coopération internationale qui tentent de coordonner la réponse des États.

Les configurations permettent de surcroît d'intégrer, dans un modèle unifié, un réseau complexe de liens d'interdépendance qui relèvent simultanément de la coopération et du conflit (Elias, 1986 : 70-71), ce qui constitue une autre caractéristique particulièrement attrayante pour l'étude des phénomènes criminels. Ceux-ci se définissent en effet par une tension constante entre des relations d'agression et de collaboration mises en œuvre par les délinquants, les victimes et leurs protecteurs. Par ailleurs, les projets et les actions de ces groupes opposés sont contraints par une vaste palette d'instruments de contrôle qui contribuent également à définir les paramètres des configurations étudiées (Elias et Dunning, 1986 : 274). En nous incitant à penser de manière intégrée comment des groupes aux intérêts diamétralement opposés sont imbriqués et inexorablement liés par des relations en équilibre mouvant ne formant qu'un seul processus, le concept de configuration permet de construire des passerelles théoriques et empiriques entre des champs d'étude qui dialoguent rarement, comme la sociologie criminelle, la gouvernance de la sécurité, la prévention situationnelle, la victimologie, ou encore les relations internationales.

Défini de manière assez générale dans *Qu'est-ce que la sociologie*, le concept de configuration s'incarne à travers des liens de nature diverse et assez peu spécifiés qui relèvent aussi bien de la dimension affective pour les groupes de taille réduite que de mécanismes politiques et économiques pour les sociétés

industrialisées et les États qui ont atteint un niveau élevé de différentiation et de stratification (Elias, 1991 : 134). Ces liens sont à distinguer des simples interactions entre individus indépendants, qui ne peuvent être définies comme des « configurations *a posteriori* » puisqu'elles ne s'inscrivent pas dans des processus de tension spécifiques (Elias et Dunning, 1986 : 273). Enfin, il faut préciser que ces liens ne traduisent pas simplement un fragile équilibre entre coopération et conflit, mais qu'ils contribuent également à illustrer comment la substance du pouvoir possède en réalité une dimension profondément relationnelle, individus et groupes l'exerçant de manière inégale, fluide, et en tirant des bénéfices fluctuants (Elias, 1991 : 131).

L'étude de l'imbrication entre coopération et conflit qu'autorise la notion de configuration ne se cantonne pas à la description statique des liens d'interdépendance qui unissent divers acteurs sociaux à un moment particulier. Au contraire, elle repose sur une approche historique qui tente de retracer les changements perpétuels et l'évolution sociale spontanée de chaque configuration afin d'en comprendre l'origine, les moments charnières, ainsi que le degré de maturité au moment de l'analyse (Elias et Dunning, 1986 : 68). Il peut sembler prématuré de raisonner en termes de longue durée dans le contexte du cybercrime, puisque la technologie qui le sous-tend s'est démocratisée il y a moins d'un quart de siècle avec la commercialisation de l'accès au Web. Toutefois, on retrouve dès le milieu des années 1960 les premières mentions des menaces à l'intégrité et à la confidentialité des données que faisaient courir les rares ordinateurs installés dans des agences gouvernementales liées à la sécurité nationale, quelques entreprises spécialisées et une poignée de centres de recherche universitaires, c'est-à-dire plusieurs décennies avant que le grand public ou les décideurs politiques ne découvrent la complexité des problèmes liés à la cybersécurité (Warner, 2012). Il est donc possible de surmonter la tyrannie du présent qui afflige trop souvent les études sur les nouvelles technologies et leur impact social pour essayer de comprendre de manière beaucoup plus évolutive comment les facteurs qui contribuent à la prolifération ou au contrôle des cybercrimes sont apparus et ont cristallisé pour former les configurations que nous observons aujourd'hui.

Si l'étude des configurations au niveau de contextes relativement circonscrits, comme des équipes de football par exemple, ne pose pas de problème empirique majeur, il en va tout autrement pour les configurations qui se déploient à l'échelle d'une région, d'une société, d'un pays ou d'un secteur d'activité économique mondialisé. De telles configurations peuvent seulement être étudiées indirectement à travers l'analyse des chaînes d'interdépendance qui les traversent et les structurent (Elias, 1991 : 131). Cette intuition, restée au stade de l'injonction dans les travaux d'Elias (Ducret, 2011), préfigure l'essor subséquent de la sociologie des réseaux. Celle-ci accorde en effet une importance particulière aux propriétés relationnelles des structures sociales, par contraste avec l'intérêt de la sociologie classique pour la catégorisation statistique des éléments qui composent ces structures. L'analyse des réseaux sociaux tire son origine des travaux initiés par Jacob Moreno sur la sociométrie durant les années 1930. Elle connaît un essor sans précédent depuis la fin des années 1990 sous l'influence des capacités de calcul accrues offertes par l'informatique

et la disponibilité de bases de données à très grande échelle (Lazega, 1994 ; Freeman, 2004 ; Watts, 2004). Parallèlement aux raffinements méthodologiques apportés à cette approche par de nombreux spécialistes des méthodes quantitatives, Manuel Castells a développé une ambitieuse réflexion théorique sur la morphologie sociale des réseaux, vecteurs privilégiés de la compréhension des phénomènes d'interdépendance économique à l'échelle mondiale.

La société en réseaux et les effets perturbateurs de la technologie

Si la notion de configuration répond à la volonté de Norbert Elias d'unifier les approches macro- et microsociologiques au sein d'un cadre analytique reposant sur le principe d'interdépendance, la théorie de la société en réseaux de Castells vise plutôt à comprendre comment les relations hiérarchiques verticales qui caractérisaient les sociétés industrielles ont été éclipsées dans les sociétés informationnelles par des relations horizontales prenant la forme de flux de données et de capitaux (Castells, 2001b). Cette prééminence du réseau comme morphologie sociale dominante est étroitement associée à la révolution technique initiée aux États-Unis au début des années 1970 par le développement et la démocratisation de l'internet. La diffusion de cette révolution numérique à l'échelle planétaire déclencha par la suite des transformations sociales et économiques caractérisées par une flexibilité inédite et une abolition des contraintes spatiales et temporelles. Comme le rappelle Castells, il ne s'agit pas de succomber par ce type d'analyses à un déterminisme technologique simplificateur, mais plutôt de prendre acte de manière empirique de l'ensemble complexe des interactions qui se nouent entre société et technique (Castells, 2001b : 27).

Les réseaux définis en tant que structures sociales ont de toute évidence préexisté à l'avènement de l'informatique et des technologies de l'information (Tilly, 2005 ; Hariri, 2015), mais ces innovations leur permettent d'exprimer un potentiel d'efficacité organisationnelle jugé supérieur à ceux de l'État ou du marché. Le réseau est défini dans cette perspective comme « un ensemble de nœuds interconnectés [où] la réalité d'un nœud dépend du type de réseau auquel il appartient » (Castells, 2001b : 576). Les nœuds ne se limitent ainsi pas à des catégories restrictives d'entités comme des individus ou des institutions : ils peuvent également représenter des lieux (un casino où se déroule une conférence annuelle d'experts en sécurité), des dispositifs techniques (des serveurs informatiques hébergeant l'infrastructure d'un réseau de pirates informatiques malveillants), ou encore des milieux d'activités humaines (comme des réseaux informels de partage du renseignement sur les cyberattaques ou des collectifs de hackers).

Si cette définition hétérogène des nœuds autorise une grande créativité théorique, elle rend assez difficile l'étude empirique systématique et la modélisation des multiples liens contingents qui les relient entre eux. Par comparaison, les études quantitatives d'analyse des réseaux sociaux se limitent en général à un seul type de liens spécifiques qui peuvent aussi bien traduire