Penser la trace dans de nouvelles échelles

Olivier RIBAUX
Professeur
École des sciences criminelles
Université de Lausanne

Les signes d'un changement d'échelle

La quiétude de la paisible commune de Rolle, située au bord du lac Léman, entre Genève et Lausanne, est perturbée durant l'été 2021, lorsque des journalistes accèdent sur le *darkweb,* librement, à des données dérobées concernant notamment plus de 5 000 administrés. L'attaque de type rançongiciel a eu lieu dans la nuit du 29 au 30 mai, mais l'incident n'a été révélé que le 20 août par le média en ligne Watson[i] Les autorités communales semblaient très empruntées quant à la manière de réagir et de communiquer. La syndique (la maire) répondait même maladroitement à la presse, dans un premier temps, qu'il s'agissait d'une « faible attaque », avant d'admettre l'ampleur du problème.

Ce genre de cas est devenu courant. Toutefois, ce qui était un problème réservé aux spécialistes est perçu maintenant directement par chacun d'entre nous. Tous les niveaux de la société sont ainsi déstabilisés. Autrement dit, nous sommes confrontés à un problème de changement d'échelles. La réaction des autorités de Rolle illustre que nous ne sommes pas vraiment préparés à affronter ces nouvelles dimensions. Les processus ne sont pas prêts.

Nous savions que toute technologie qui s'intègre dans nos activités routinières cause des transformations profondes. De l'imprimerie à l'automobile, en passant par le téléphone, la radio ou la télévision, toutes ces innovations ont bousculé nos sociétés. Nous avons toutefois eu besoin d'années de recul pour prendre la mesure de ces bouleversements, puis pour retrouver de la tranquillité. Des effets de bord imprévus et désagréables ont chaque fois été rendus visibles lorsque les ordres de grandeur ont changé. Nous sommes maintenant dans cette situation. Nous sommes un peu désemparés, car nous manquons de distance.

Il faut se dépêcher pour réagir puisque nous avons déjà raté la période qui aurait pu nous permettre d'anticiper. Dans un cheminement difficile, nous proposons d'abord d'apprendre à penser dans ces nouvelles échelles.

Une représentation du problème

Pour prendre la mesure de l'ampleur du défi, construisons une image qui rend la situation plus intelligible. Le modèle des cinq « V » du *big data* peut constituer une base[ii]. Cette approche est archiconnue et peut paraître trop élémentaire pour le lecteur. Mais je ne suis pas sûr qu'il soit toujours bien compris pour son potentiel à nous aider à penser les échelles. Nous sommes en effet toutes et tous d'accord que nous vivons dans un espace avec quelques « 0 » de plus qu'il n'y a pas si longtemps, sur chacune des dimensions du modèle. Ce constat est notamment évident lorsque nous parlons des **V**olumes de données qui représentent massivement des textes, des images, du son, ou des flux vidéo : des unités comme le Petaoctet, voire l'Exaoctet ou le Zettaoctet ne nous impressionnent plus. La **V**ariété de ces données s'est bien sûr aussi étendue considérablement. Pensons à la diversité des traces numériques que nos activités quotidiennes produisent par l'utilisation des objets connectés et qui sont exigées pour évoluer dans notre société. Dans le modèle, la grandeur suivante exprime la **V**élocité, pour garder le « V » de l'anglais ***V**elocity*, qui nous renvoie à l'échelle temporelle des traitements. À l'inverse des autres « V » en expansion, cette dimension se réduit, mais aussi en ordre de grandeur : possibilités d'exploiter de gigantesques quantités traces à une vitesse difficile à concevoir et nécessité de déléguer à un ordinateur de nombreuses tâches rendues irréalistes pour un être humain. Par exemple, la sécurité de beaucoup de systèmes d'information dépend directement de l'instantanéité de la détection des attaques informatiques par des méthodes qui relèvent de l'intelligence artificielle.

Le « V » suivant renvoie à la **V**aleur des données. Cette grandeur n'est pas seulement économique, elle est aussi morale et fait référence aux libertés fondamentales. Nous ne sommes pas au bout de nos peines pour intégrer dans une juste mesure les principes de la protection des données, ni même pour évaluer correctement cette valeur. C'est lorsqu'on se les fait voler ou qu'elles sont rendues inaccessibles par malveillance, par une panne ou par une erreur de manipulation qu'on se rend vraiment compte de cette valeur. La dernière dimension porte sur la **V**éracité : inutile de s'arrêter sur la qualité de l'information qui circule par les réseaux.

Nous sommes déjà convaincus des bouleversements d'échelles sur chacune de ces grandeurs. Imaginons-les maintenant dans un référentiel à cinq dimensions qui dépendent chacune l'une de l'autre, lui-même à considérer dans un écosystème composé d'objets connectés par des réseaux et d'êtres humains. Nous nous plongeons alors dans un espace complètement inconnu, car il doit être pensé à une échelle et à un degré de complexité dont nous n'avons pas l'habitude et pour lesquels nous ne sommes pas forcément constitués naturellement. L'incertitude y règne : on n'y maîtrise pas tout.

Pour mieux percevoir ces bouleversements, on peut aussi se

souvenir d'un passé pas si lointain, mais déjà considéré comme ridicule par les jeunes générations. Mon premier Macintosh faisait fonctionner tant bien que mal un ensemble très réduit d'applications basiques, sans disque dur sur un système d'exploitation qui tenait sur une disquette de 640K. Il n'y a finalement pas si « longtemps » puisque c'est encore à vue humaine. On dit qu'une telle évolution a quelque chose d'exponentiel. Ce terme emprunté aux mathématiques est toujours plus utilisé dans le langage courant. Nous avons besoin de cette notion pour exprimer que la progression n'a rien de linéaire : il ne suffit donc pas d'étendre nos anciennes conceptions à la nouvelle situation, car nous sommes projetés dans un espace d'une autre complexité. Nous pouvons maintenant comprendre que, dans ce monde à explorer, plein de promesses, mais aussi de dangers, empiler des normes de sécurité ne suffira clairement pas. Les vieilles recettes peuvent avoir quelques vertus, mais leurs effets resteront limités, car, avec les échelles, c'est la nature des choses qui changent.

Admettre sans paniquer

En apprenant à penser dans de nouveaux ordres de grandeur, nous nous mettons dans de meilleures conditions pour reconnaître l'ampleur du problème. Mais nous allons alors prendre conscience de dangers. Cela ne nous arrange pas et explique les résistances farouches face à des évidences. Comment justifier de remettre en cause, même modestement, notre confort numérique, alors que notre quotidien, nos habitudes, nos loisirs et l'économie en dépendent tellement ?

Les expériences réalisées avec d'autres technologies, pourtant à une échelle réduite, l'ont déjà démontré. Le nombre de morts sur la route provoqué par l'automobile a diminué, mais il subsiste nécessairement des décès : malgré l'évidence, nous ne voulons pas admettre que l'être humain n'est pas physiquement constitué pour se déplacer à la vitesse d'une automobile. On peut contrôler, atténuer les risques, mais il y aura toujours des drames causés par la route, même si chacun d'eux est « inadmissible ».

Concrètement, reconnaître humblement que nous sommes propulsés dans un écosystème complexe plein d'incertitudes pour lequel nous ne sommes pas constitués, c'est donc aussi apprendre à vivre avec l'imprévu et le danger. Cette attitude est toutefois en tension avec l'analyse d'Ulrich Beck[iii]. Bien avant l'émergence du big data, ce dernier concevait déjà une évolution d'une «société du risque » qui veut obstinément tendre vers l'impossible « risque zéro ». Si Beck a raison, dans notre nouveau contexte, la panique qui peut résulter d'une perception de risques toujours plus nombreux (en ordre de grandeur) et impossibles à maîtriser, constitue un nouveau risque réel pour la sécurité. Une théorie criminologique nous dit bien que l'insécurité peut entraîner l'insécurité dans un cercle vicieux. L'étape suivante consiste donc à identifier les façons d'atténuer ces inquiétudes.

Vivre avec les nouveaux risques

Par exemple, Dominique Boullier, en se référant à Gérard Berry, rend compte de l'inévitable « bug » qui résulte de la production de systèmes informatisés complexes :

« Le « bug » n'est ni un produit de l'erreur humaine ni un effet d'une quelconque mauvaise intention ou d'économies abusives sur les coûts de développement. Le bug est constitutif de l'informatique des systèmes complexes »[iv].

Les grandes institutions comprennent progressivement le fait que le bug, aux conséquences parfois désastreuses, est aussi inévitable, impossible à éradiquer dans notre nouvel espace complexe, que les morts sur la route. Cela ne veut pas dire qu'on ne peut rien faire : le succès des programmes de type *bug bounty* qui consistent à soumettre volontairement les logiciels aux assauts de hackers indique les possibilités de vivre avec le risque, tout en tentant d'en atténuer les effets ou rendre plus rare son actualisation.

Dans cette constellation de changements d'échelles, toute une variété de réponses qui vont dans notre sens semblent toutefois émerger.

La notion de risque est forcément liée à l'émergence d'assurances qui offrent toujours davantage de prestations. Qui veut exploiter des données se fait maintenant vite questionner sur la proportionnalité, la nécessité et la transparence des traitements prévus, surtout en matière judiciaire et dans l'économie. Ces concepts fondamentaux de la protection des données s'intègrent concrètement dans nos systèmes d'information. Au-delà, le débat éthique se renforce. La prévention s'organise aussi : les écoles élaborent des programmes d'«hygiène numérique ». Dans différentes organisations, on sensibilise toutes les collaboratrices et tous les collaborateurs à la responsabilité qu'ils ont en tant que gardien·ne des données produites et gérées par l'institution. Sur les plans managériaux et techniques, les standards en matière de cybersécurité, au sens large, se consolident. Le suivi des attaques et des modes opératoires à l'échelle mondiale devient systématique. En milieu judiciaire, les enquêteurs savent exploiter les erreurs commises par des malfaiteurs, eux aussi dépassés par la complexité des systèmes et producteurs inconscients de traces. La sécurité s'intègre directement dans la conception de base des systèmes. Les formations en cybersécurité prolifèrent et la recherche s'active. Des ressources et de nouveaux moyens sont dégagés.

En matière de réponses, des piliers se construisent donc indéniablement. Toutefois, nous avons le sentiment que ces approches restent très cloisonnées : chacune et chacun reste dans son champ de spécialité pour étendre son approche traditionnelle aux questions numériques, par analogie. Quelle est alors la solidité de l'édifice ?

L'interdisciplinarité

L'analyse des ordres de grandeur nous incite à aborder les nouveaux problèmes en sortant des carcans disciplinaires traditionnels. Ces derniers distribuaient

relativement bien le travail dans nos sociétés plus simples. Ils sont en revanche inopérants dans les nouveaux espaces esquissés. Nous ne sommes pas assez « indisciplinés » pour répondre à l'ampleur des changements et aux enjeux. L'interdisciplinarité est souvent affirmée et revendiquée, mais en fait très peu comprise et appliquée. Dans un domaine que nous connaissons bien dans notre École, nous constatons par exemple que l'intégration de la cybersécurité et des poursuites judiciaires n'est de très loin pas aboutie dans les pratiques, la recherche et la formation. L'articulation est pleine de malentendus. La notion de trace, qui peut pourtant jouer un rôle pivot tant elle est au centre des activités humaines et de la question des ordres de grandeur, devrait davantage rassembler en vue de construire une plateforme propice au développement de visions plus intégrées. C'est le rôle de la science forensique.

Boullier analyse cette situation, une fois de plus, avec pertinence : « Les systèmes institutionnels ont permis de maintenir la valorisation des disciplines alors que les questions qui présentent un intérêt sont nécessairement interdisciplinaires. Cette situation est d'autant plus dommageable qu'elle éclipse quiconque travaille à la frontière de deux champs disciplinaires »[v]. Nous avons vécu cela dans les premières années d'une formation interfacultaire de Maîtrise universitaire en droit, criminalité et sécurité des technologies de l'information que nous avions lancée avec des partenaires juristes et en sécurité des systèmes d'information, il y a presque vingt ans. Elle a été ignorée par le système universitaire durant de nombreuses années pour ne prendre un véritable envol que maintenant.

Conclusion

En bref, admettons d'abord les changements d'échelles pour prendre la mesure des enjeux et modifier notre manière de penser. Adoptons simultanément des attitudes courageuses en faisant face aux risques. Enfin, conceptualisons autour de la trace pour construire des visions stratégiques et des réponses opérationnelles réalistes, plus proactives et effectivement inter-disciplinaires. À ce titre, la science forensique, en tant que discipline, doit être davantage reconnue.

Mais dépêchons-nous.

[i] https://www.watson.ch/fr/suisse/vaud/323755680-vaud-rolle-a-ete-piratee-par-des-hackers-donnees-volees-sur-le-darknet

[ii] BOURANY, T. 2018. Les 5V du big data. Regards croisés sur l'économie, 23, 27-31.

[iii] Ulrich Beck. La société du risque. Sur la voie d'une autre modernité. Aubier, 2001

[iv] Boullier, Dominique. Sociologie du numérique. Armand Colin. Édition du Kindle, 2016, p 24

[v] Dominique Boullier, Jacques Athanase Gilbert, Daphné Vignon, Armen Khatchatouro. Le grand entretien avec Dominique Boullier, Etudes digitales, Classiques Garnier, p. 247