

Quelle sécurité dans un monde numérisé post-Covid ?

La pandémie Covid-19 a propulsé le monde dans une vie professionnelle et sociale essentiellement interconnectée : travail, médecine, école, administration, presse, réunions etc ... Cependant, la pratique à montrer l'impact aussi sur la vie personnelle, amicale et familiale comme les concerts, anniversaires ou apéritifs confinés se partageant aussi par messagerie et visio. Ainsi, la plus grande partie des entreprises, administrations et population, même réfractaires ou mal équipées, ont découvert les bienfaits du numérique. Mais sommes nous vraiment plus en sécurité, dans ce nouveau monde ?

Certes, moins de risque de contamination et d'agression mais la délinquance s'adapte à cette nouvelle forme d'organisation et les forces de sécurité doivent donc évoluer aussi.

Eléments contextuels :

Cette épidémie mondiale Covid-19, a confiné une partie de la population des villes ou des campagnes, dans un nouvel univers de : télétravail, téléenseignement, télé-médecine, télé-administration, télé-marketing ..., aujourd'hui, à Paris, même les tickets de bus ne sont plus vendus à bord par les chauffeurs mais par SMS, les clients évitent la monnaie et payent par carte sans contact, les visioconférences ne sont plus réservées aux cadres mais régulières entre amis ou parents. La vie s'organise autour de services modulaires intégrés, connectés et interopérables.

La peste de Camus semble dépassée. Aujourd'hui, sans connexion point de salut ! En conséquence, l'illlectronisme, les fractures sociales et territoriales deviennent des enjeux de société et de résilience ; mais quid de la sécurité ?

De fait, ces nouvelles technologies induisent des effets sociaux, politiques et éthiques comme criminels.

Selon les penseurs déterministes, adeptes de l'universalisme, comme **John von Neuman**, mathématicien américain d'origine hongroise, acteur de l'élaboration de la théorie des ensembles, à la conception de la bombe H, et précurseur de l'intelligence artificielle et des sciences cognitives, **la technique est la « représentation par excellence du progrès »** ... Elle n'est pas seulement un instrument de la modernité, mais le moteur même du système social ».

Alors qu'au contraire pour les essentialistes, **Jacques Ellul**, historien du droit, sociologue et théologien protestant libertaire français, penseur de la technique comme une aliénation de l'homme du XXe siècle ou pour **Martin Heidegger** la considérant au plan humain, comme **une menace pour la « survie spirituelle ainsi que matérielle »**.

Jürgen Habermas, théoricien allemand en philosophie et en sciences sociales, issu de la deuxième génération de l'École de Francfort, essaya de réconcilier ces deux pensées en combinant le matérialisme historique de Marx avec le pragmatisme américain. Néanmoins les concepts liberticides européens de la technologie vont impacter les retards de croissances économiques et industrielles dans le domaine laissant le champs libre aux visions américaines et asiatiques pour investir dans la recherches et le développement.

Néanmoins, face à la multiplication des usages et des dérives, les forces de sécurité chargées d'assurer la protection des personnes et des biens, de veiller à la tranquillité, à la sécurité publique et au maintien de l'ordre public, n'ont pas manqué cette évolution technologique sociétale.

Certes, au plan sanitaire, un monde digitalisé entraîne moins de contacts corporels, moins de monde dans les transports, les lieux communs de travail ou d'école et donc moins de risque de contagion. Néanmoins au détriment des relations humaines, du moral individuel et de la sociabilité, souvent facteurs essentiels de guérison, de vouloir vivre et de partage. De plus les atermoiements sur l'application STOPCOVID laisse présager que la

traçabilité socialement acceptée pour faire des rencontres ou des échanges sociaux aux mains d'entreprises commerciales aux risques d'atteinte à la vie privée, reste majoritairement refusée pour assurer la sécurité sanitaire de la population.

Une évolution vers une réflexion sociale d'une cyber culture s'impose sur une autre théorie que celle édiflée sur la peur d'un Big brother étatique issu du fameux livre 1984 de Georges Orwell, totalement dépassé par la réalité des GAFAM ((Google, Amazon, Facebook, Apple, Microsoft) et BATX (Baidu, Alibaba, Tencent et Xiaomi). A Taïwan, le respect du confinement par les personnes malades est vérifié directement par le biais des données mobiles, sans manifestation ou désordre public pour atteinte aux libertés.

Au niveau de la délinquance, à l'évidence moins de monde dans les rues réduit les agressions de voie publique mais accroît les violences conjugales et familiales. Le trafic de stupéfiant bénéficie du système avec commandes sur les réseaux et délivrance par livreur à domicile. Les escroqueries et trafics sur le Net évoluent vers les masques et le gel et si les cambriolages diminuent dans les maisons habitées, il a fallu escorter les livraisons des hôpitaux attaquées à mains armées comme des transports de fond.

La naissance d'une police moderne :

De fait, les forces de sécurité évoluent vers le numérique:

- cyber patrouilles sur le Net et drones (surveillances des lieux publics et attroupements lors du confinement)
- cyber surveillance du Net et signalement citoyens : www.internet-signalement.gouv.fr
- e-commissariat et plainte en ligne : www.pre-plainte-en-ligne.gouv.fr
- veille cybernétique et cyber-attaques : www.cybermalveillance.gouv.fr
- messagerie Tchat pour répondre aux questions sur les formalités (formulaires) : www.police-nationale.interieur.gouv.fr
- vidéo-protection et détection des absences de masques
- contrôles d'identité et formulaires numériques via des lecteurs ou des smartphones
- constatations, contrôles et rédactions via des tablettes (NEOGEND et NEOPOL)
- Fichiers internationaux Interpol, Europol et Shengen.

Les limites conjoncturelles :

Cependant, ces évolutions restent mineures face aux développements actuels de la criminalité organisée mondialisée et interconnectée. Ces dernières adaptations des forces de sécurité, effectuées au coup par coup, nécessitent une plus grande **planification** avec une **combinaison d'ensemble des moyens financiers, humains et matériels**, ainsi qu'une **cohérence et interopérabilité des techniques, des métiers, du recrutement, de la formation, de la gestion et de l'organisation avec des chaînes hiérarchiques plus courtes et des échanges horizontaux entre services**, dans un monde interdépendant, complexe et rapide, où les vidéo et capitaux font le tour de la planète en quelques clics et quelques secondes.

De plus, la conjoncture mondiale n'apparaît pas favorable aux pays européens, handicapés par leurs freins culturels et libéraux jusqu'au-boutistes entraînant un **retard technologique** où tous les logiciels sécuritaires sont anglo-saxon et tous les équipements électroniques sont d'origine asiatique. De même, sur les **usages** les craintes liberticides sociétales s'avèrent risquées. Ainsi, quand des grands pays comme le Russie, la Chine, l'Inde, les Etats-Unis et l'le Royaume-Unis¹ utilisent la reconnaissance faciale et la biométrie à l'entrée de leur territoire et pour

¹ « Le Metropolitan Police Service (Met), force de police principale du Grand Londres, a commencé à se servir de la reconnaissance faciale en direct afin de détecter les personnes recherchées par les autorités britanniques, selon ce que rapporte the Metropolitan police commissioner, Cressida Dick au journal The Guardian. »,

lutter contre toutes sortes de délinquance, fraudes identitaires et déviances, **l'Europe ne peut qu'apparaître comme un territoire ouvert aux quatre vents de tous les terroristes et trafiquants** qui n'ont aucune raison de voyager avec une identité exacte (nom, prénom date de naissance contrôles Schengen actuels) venant de pays ou un vrai passeport avec une fausse identité se monnaie pour quelques euros.

Le défi des « smart cities » ou « villes intelligentes » :

Grâce aux progrès de l'Intelligence Artificielle due au Machine Learning, la propension de gérer les données variées, volumineuses et non structurées (Big Data), les capacités de stockage démesurée du Cloud Computing, des systèmes de gestion vidéo avec reconnaissance faciale, le développement des capteurs et des objets interconnectés à des réseaux de plus en plus performants, la technologie offre aux citoyens des perspectives d'amélioration de **qualité de vie** de plus en plus recherchées au point que le choix d'un logement se fait sur des critères numériques autant que d'environnement.

La sécurité fait partie intégrante de ce nouveau concept de bien-être numérique impactant fortement le fonctionnement actuel des **services publics et privés vers un travail plus collaboratif**.

Pour assurer la sécurité d'une ville entière, les forces de sécurité se doivent d'accéder aux différents systèmes informatiques qui s'intègrent et communiquent entre eux avec une infrastructure partagée, de capteurs connectés à un réseau commun et gérés par plusieurs entités : parfois plusieurs municipalités en communauté, services publics (circulation, distribution eaux, nettoyage), services privés : (électricité, transports, centres commerciaux). La vision purement régalienne de la sécurité doit être abandonnée pour un nouveau paradigme. Toutes les organisations et services doivent délaisser le fonctionnement en silo et impose de travailler en partenariat dans un écosystème de contributeurs pour atteindre **l'objectif commun de la tranquillité et de quiétude de citoyens confiants et exigeants**.



<https://www.theguardian.com/technology/2020/feb/24/met-police-chief-cressida-dick-facial-recognition-technology-critics-ill-informed>

² Illustration du projet de capteurs sonores à Saint-Etienne – Serenicity <https://www.demainlaville.com/safe-city-lanonimat-dans-la-ville-est-en-train-de-sevanouir/>

La cyber résilience :

Néanmoins, la version idyllique numérique ne résiste pas à la réalité de l'imagination de la délinquance. Ainsi la nouvelle cybercriminalité rapporte aujourd'hui plus de gain que le trafic de stupéfiant.

Maitrise, Management et contrôle :

Ce nouvel univers numérique n'est pas sans conséquences professionnelles, éthiques, juridiques et sociales pour les forces de l'ordre. Ce monde hyper connecté et sans frontières, basé sur des équipements extérieurs impacte les missions quotidiennement des forces de l'ordre. En effet, exploitées en temps réel ou a posteriori, les données générées par ces dispositifs connectés constituent autant de traces et de preuves des activités de leurs utilisateurs.³

³ <https://sd-magazine.com/securite-numerique-cybersecurite/les-objets-connectes-au-service-de-la-police-judiciaire>