



REVUE DU DROIT DES AFFAIRES EN AFRIQUE (RDAA)

Editée par

L'Institut du droit d'expression et d'inspiration françaises

Regard, Mai 2020

REGARD

Par

KOUMAKO Yao Justin

Juriste internationaliste - Cybersécurité

LES ENJEUX CYBER DU COVID-19



REVUE DU DROIT DES AFFAIRES EN AFRIQUE (RDAA)

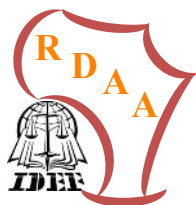
Editée par

L'Institut du droit d'expression et d'inspiration françaises

Regard, Mai 2020

Sommaire

- Résumé en français et en anglais / Référence de l'article
- Article
- Note biographique de l'auteur



Regard, Mai 2020

Résumé

L'humain est au cœur de la cybersécurité ; acteur incontournable et maillon faible d'une chaîne complexe car « *derrière les machines se trouvent des utilisateurs et des acteurs* ». Plus affaibli que jamais par l'irruption soudaine et violente du COVID-19, il se retrouve enrôlé dans des enjeux cyber à plusieurs vitesses. A la vérité, le COVID-19 a occasionné une utilisation accrue du numérique. De certains Etats qui utilisent des drones à des fins de sensibilisation, de désinfection des routes aux particuliers contraints à faire du télétravail, le numérique n'a jamais été aussi prégnant. Cette utilisation accrue du numérique n'est pas sans conséquences car qui dit utilisation accrue du numérique dit augmentation sévère de cyberrisques. S'il est vrai que la cybermenace est permanente et que la « cyberpaix » n'existe pas, les tentatives d'intrusions informatiques par les acteurs étatiques et les actes de cybermalveillances d'autres acteurs dans une période qualifiée de « guerre sanitaire » soulèvent sans aucun doute des questions juridiques d'actualité brûlante qu'il convient de bien poser et de traiter. Quelles sont les cyberattaques à l'heure du coronavirus ? Par ailleurs, évoquer l'humain, c'est évoquer également ses droits. Quelle protection juridique des données personnelles en général et des données sensibles en particulier en cette période ?

Abstract

The human being is at the heart of cybersecurity; a key player and a weakest part of a complex chain because "behind the machines are users and participants / protagonists". Weakened more than ever by the sudden and violent eruption of COVID-19, it finds itself involved in multi-speed cyber issues. Indeed, COVID-19 has led to an increased use of digital technology. From some States using drones to raise awareness, road disinfection to individuals forced to work from home, digital has never been more prevalent. This increased use of digital technology is not without consequences, because it means a severe increase in cyber-risks. While it is true that the cyber threat is permanent and that "cyber peace" does not exist, attempts at computer intrusion by State actors and the cyber-malicious acts of other actors in a period described as a "health war" undoubtedly raise topical legal questions that must be properly identified and dealt with. What are the cyber-attacks in the age of the coronavirus? Moreover, referring to human being triggers the question of its rights. What is the legal protection of personal data in general and sensitive data in particular at this time?

Référence pour citer l'article :

RDAA, Regard Mai 2020 – « Les enjeux cyber du COVID 19 », KOUMAKO Yao Justin,
<http://www.institut-idef.org>



Regard, Mai 2020

L'humain est au cœur de la cybersécurité¹ ; acteur incontournable et maillon faible d'une chaîne complexe car « *derrière les machines se trouvent des utilisateurs et des acteurs* »². Plus affaibli que jamais par l'irruption soudaine et violente du COVID-19, il se retrouve enrôlé dans des enjeux cyber à plusieurs vitesses. A la vérité, le COVID-19 a occasionné une utilisation accrue du numérique. De certains Etats qui utilisent des drones à des fins de sensibilisation, de désinfection³ des routes aux particuliers contraints à faire du télétravail, le numérique n'a jamais été aussi prégnant. Cette utilisation accrue du numérique n'est pas sans conséquences car qui dit utilisation accrue du numérique dit augmentation sévère de cyberrisques. S'il est vrai que la cybermenace est permanente et que la « cyberpaix » n'existe pas, les tentatives d'intrusions informatiques par les acteurs étatiques et les actes de cybermalveillances d'autres acteurs dans une période qualifiée de « guerre sanitaire »⁴ soulèvent sans aucun doute des questions juridiques d'actualité brûlante qu'il convient de bien poser et de traiter.

En effet l'actualité du numérique à l'heure du COVID-19 est empreinte de cyberattaques dont les motivations sont variées. Quoi qu'il en soit, les données personnelles figurent également au cœur des débats tant elles sont massivement générées en ligne et la question de leur protection n'est pas sans faire couler d'encre.

Il n'existe pas en droit international une définition conventionnelle d'une cyberattaque. Selon le Lexique sur le cyberspace, c'est un « *terme générique qui désigne une attaque informatique. Largement utilisé, ce terme recouvre en fait plusieurs réalités, plusieurs types d'attaques de nature et aux conséquences très diverses comme le « défacement », les attaques en déni de service ou logiciel malveillant, ou encore des attaques à but d'espionnage ou de sabotage. Le terme cyberattaque peut ainsi faire référence à une technique d'attaque en elle-même ou un objectif de l'attaquant* »⁵. A défaut d'une définition consensuelle, les Etats définissent le terme « cyberattaque » de manières variées. Ainsi selon la France, une cyberattaque est une « *Action volontaire, offensive et malveillante, menée au travers du cyberspace et destinée à*

¹ YUKSEL (A.), « Remettre l'humain au cœur de la cybersécurité », *Revue de la gendarmerie nationale*, Décembre 2019, n° 266

² CATTARUZZA (A.), DANET (D.), TAILLAT (S.), *La cyberdéfense. Politique de l'espace numérique*, Armand Colin, 2018

³ En Chine, des drones agricoles ont été mobilisés pour désinfecter des routes ou même certains hôpitaux.

⁴ Dans son discours télévisé du 16 Mars 2020 sur le COVID-19 en France, le président français E. MACRON déclare : « Nous sommes en guerre, en guerre sanitaire, certes : nous ne luttons ni contre une armée, ni contre une autre Nation. Mais l'ennemi est là, invisible, insaisissable, qui progresse. Et cela requiert notre mobilisation générale ».

⁵ Desforges, Alix, et Enguerrand Déterville. « Lexique sur le cyberspace », *Hérodote*, vol. 152-153, no. 1, 2014, pp. 22-25.



Regard, Mai 2020

provoquer un dommage (en disponibilité, intégrité ou confidentialité) aux informations ou aux systèmes qui les traitent, pouvant ainsi nuire aux activités dont ils sont le support »⁶.

Les données personnelles, quant à elles, sont définies par l'article 4 §1 du RGPD⁷. Cette définition qui peut prétendre à l'exhaustivité mérite d'être retenue dans le cadre de la présente étude.

Quelles sont les cyberattaques à l'heure du coronavirus ? Quelle protection juridique des données personnelles en général et des données sensibles en particulier en cette période ?

La réponse à ces questions implique une approche interdisciplinaire car contenant des aspects de droit pénal, droit européen et international. Fort de cela, il est convenable de voir dans une première partie la recrudescence des actes de cybermalveillances (I) avant de voir dans une seconde partie l'incidence du COVID-19 sur la protection des données personnelles (II).

I. La recrudescence des actes de cybermalveillances

Le COVID-19 induit largement la réussite des actes d'intrusions informatiques des cybercriminels. En cela, il est une nouvelle aubaine de la cybercriminalité (A). Le comportement des Etats dans le cyberspace à l'heure où le COVID-19 sévit éprouve également les relations internationales (B).

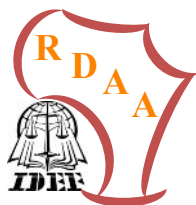
A. Le COVID-19, la nouvelle aubaine de la cybercriminalité

Dans un communiqué joint en date du 20 Mars 2020, plusieurs institutions européennes (commission, ENISA, EUROPOL, CERTEU) alertent que des acteurs malveillants exploitent les circonstances exceptionnelles du COVID-19 pour faire des cyberattaques ciblées. Ces attaques sont diverses et ont pour cible de simples télétravailleurs, des hôpitaux ou mêmes des Etats et des organismes internationaux. Myriam Quémener et Clément Wierre notent que « *Le phénomène n'est pas nouveau : que ce soit le tsunami de 2004 en Asie ou le tremblement de terre en Haïti de 2010, les grandes catastrophes sont systématiquement exploitées par les cybercriminels à des fins pécuniaires ou d'espionnage* »⁸.

⁶ France, Glossaire interarmées de terminologie opérationnelle (GIATO) N° 212/DEF/CICDE/NP du 16 décembre 2013

⁷ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Article 4 §1 : « Aux fins du présent règlement, on entend par : «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale; »

⁸ QUEMENER(M.), WIERRE (C.), Les cyberattaques à l'heure du coronavirus, Dalloz actualités, 21 Mars 2020.



Regard, Mai 2020

L'on peut noter ainsi des attaques par hameçonnage avec pour but d'exfiltrer, grâce à des liens contenus dans des mails ou messages, des données sensibles notamment bancaires à leurs cibles. Pour atteindre ces objectifs, les attaquants ont recours à des moyens divers. Il s'agit entre autres d'usurpation d'identité d'organisations à des fins de propositions de service moyennant une somme payable en ligne. Au début de la crise en France par exemple, des pseudo-sites officiels ont proposé aux populations confinées le pré-remplissage en ligne de l'attestation sur l'honneur⁹. Or au début du confinement, pour être valide devant les autorités de sécurité, ladite attestation n'est qu'à télécharger et remplie à la main ou être rédigée intégralement de façon manuscrite. Le formulaire numérique avec le QR code¹⁰ n'est qu'une actualisation récente du ministère de l'intérieur. D'aucuns proposent des marchandises¹¹ qui ne seront jamais livrées. C'est donc à ces fins qu'il y a une augmentation de l'enregistrement de noms de domaine pour surfer sur la vague sanitaire.

Au rang des attaques, on note également les *ransomware* ou rançongiciels¹². Il s'agit de virus qui cryptent les données de la cible visée. Les attaquants en profitent alors pour faire du chantage : les données contre le paiement d'une rançon. Les *ransomware* les plus connus sont Wannacry et NotPetya. A l'heure actuelle, il n'y a pas de chiffres officiels sur ces types d'attaques. L'urgence sanitaire semble l'emporter sur la vigilance informatique. Ces cyberattaques sont cependant des menaces réelles et non-négligeables.

En ce qui concerne les entreprises, en sus d'être les cibles des attaques susmentionnées, elles sont des cibles privilégiées d'attaques comme les faux ordres de virement ou encore la Fraude au président¹³. En Chine où le COVID-19 a fait ses premières apparitions, la Commission chinoise de réglementation des banques et des assurances a signalé plusieurs arnaques qui ont

⁹ En France, il est interdit de circuler en dehors du domicile depuis le 17 Mars 2020. Cette interdiction connaît tout de même des exceptions. L'attestation sur l'honneur est le document qui permet aux citoyens de se prévaloir des exceptions légales pour leur déplacement en dehors de leur déplacement pendant la période de confinement.

¹⁰ Quick Response Code. Il s'agit d'un code-barres en deux dimensions, constitué de modules noirs disposés dans un carré à fond blanc. Il permet un décodage rapide via un lecteur de code-barres ou un smartphone.

¹¹ Il s'agit notamment de marchandises en pénurie à cause de la crise sanitaire comme les masques ou encore des gels hydro-alcooliques

¹² Dominique Filipone, Le ransomware visant Marseille perturbe le décompte des décès du COVID-19, Le Monde Informatique, 06/04/2020

¹³ La Fraude au président ou encore fraude aux ordres de virement (FOVI) est une escroquerie qui consiste, pour l'escroc, à se faire passer pour le dirigeant d'une entreprise et à obtenir un virement, de la part d'un des employés de l'entreprise, vers un compte en banque souvent situé à l'étranger.



Regard, Mai 2020

touché des banques nationales.¹⁴

La convention de Budapest sur la cybercriminalité du Conseil de l'Europe définit le cadre juridique de lutte contre la cybercriminalité en Europe et bien au-delà des frontières européennes car étant ouverte à l'adhésion d'Etats non membres du Conseil de l'Europe. Elle fait obligation aux Etats d'ériger en infractions pénales les crimes commis à base d'outils informatiques. La France a signé et ratifié cet instrument de répressions de crimes informatiques. Il est, pour l'heure, l'instrument international de répression de la cybercriminalité par excellence. Cependant la cybercriminalité par sa nature transfrontière interroge encore sur l'efficacité de la répression.

Dans un tel contexte, il vaut mieux prévenir les attaques cybercriminelles. Ce travail préventif est fortement porté par des institutions qui, par leur travail, aident les internautes à éviter l'ouverture de failles sur leurs outils informatiques. En France par exemple, l'ANSSI¹⁵ a récemment publié un guide du nomadisme numérique. Le site gouvernemental cybermalveillance.gouv.fr informe également les entreprises, les particuliers et les collectivités sur les cybermenaces et leur donne les moyens de s'en défendre.

Les cyberattaques à des fins criminelles sont pénalement répréhensibles mais si elles sont attribuables à un Etat, elles peuvent soulever de sérieuses questions de droit international et le COVID-19 en offre d'excellentes occasions.

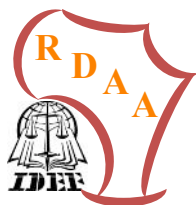
B. Les relations internationales à l'épreuve des cyberattaques liées au COVID-19

Il faut reconnaître a priori que le COVID-19 ne semble pas ébranler les relations internationales bien que le Conseil de Sécurité reste, pour l'heure, divisé lors de sa première réunion sur le virus. Son apparition semble d'ailleurs réunir l'humanité contre un unique ennemi, l'invisible Corona virus disease-2019. Les Etats font preuve d'une solidarité internationale qui va au-delà des clivages idéologiques qui les opposent souvent dans les grandes arènes internationales¹⁶.

¹⁴ Florian Dèbes, Les cyberattaques capitalisent sur le coronavirus, Les échos, 11/03/2020, consulté en ligne le 21/03/2020 [https://www.lesechos.fr/tech-medias/hightech/les-cyberattaques-capitalisent-sur-le-coronavirus-1184259]

¹⁵ Agence nationale de sécurité des systèmes d'informations

¹⁶ Face à la montée en puissance du virus en Italie, le Cuba, la Russie, et la Chine lui ont prêté mains fortes. Le Cuba a envoyé 52 médecins pour aider leurs collègues italiens. La Russie a annoncé l'envoi d'une centaine de virologues militaires en Italie. La Chine a envoyé neuf experts médicaux et plusieurs tonnes de matériel.



Editée par

L'Institut du droit d'expression et d'inspiration françaises

Regard, Mai 2020

Cette solidarité internationale peut, cependant, n'être que l'arbre qui cache la forêt notamment en ce qui concerne le comportement des Etats dans le cyberspace. A l'heure où la pandémie sévit dans plusieurs Etats et où toute l'attention reste focalisée sur elle, les cyberattaques peuvent se révéler de puissants outils entre les mains des Etats et devenir « *une source majeure de tensions entre les Etats* »¹⁷ alors même que la pandémie est susceptible d'être qualifiée de menace contre la paix et la sécurité internationales¹⁸. On dénombre ainsi plusieurs cyberattaques ayant lien avec le COVID-19. De ce point de vue, un exemple saillant mérite d'être pris pour entretenir la réflexion.

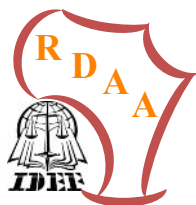
Une cyberattaque aurait visé les Etats-Unis et particulièrement les infrastructures informatiques du Health and Human Services Department (HHS)¹⁹. Il s'agirait d'une attaque Ddos²⁰. La cyberattaque qui aurait visé l'agence américaine de la santé aurait ainsi pour but de ralentir ses systèmes d'information. Vraisemblablement, les sources de cette attaque restent inconnues. Les responsables du HHS ont assuré qu'ils n'ont eu aucune dégradation de donnée et suspectent que l'attaque serait d'origine étatique sans donner davantage de précision à ce propos. Cela pose bien évidemment des problèmes de droit international notamment celui de

¹⁷ Karine BANNELIER-CHRISTAKIS, *Les cyberattaques toujours plus puissantes et plus sophistiquées constituent désormais une source majeure de tensions entre les Etats*, (H)Auteurs n°4, 29/01/2018, consulté le 24/03/2020 [<https://newsroom.univ-grenoble-alpes.fr/h-auteurs/numero-4/les-cyberattaques-toujours-plus-puissantes-et-plus-sophistiquees-constituent-desormais-une-source-majeure-de-tensions-entre-les-etats--299484.kjsp>]

¹⁸ « Covid-19 is menacing the whole of humanity...and so the whole of humanity must fight back », Antonio GUTERRES, secrétaire général des Nations Unies lors du lancement du « Global Humanitarian Response Plan »

¹⁹ STEIN (S.), JACOBS (J.), Cyber-attack hits US Health Agency Amid COVID-19 Outbreak, 16/03/2020, consulté le 24/03/2020 [<https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-9-response>]

²⁰ Selon le Lexique sur le cyberspace d'Alix Desforges et Enguerrand Déterville, une attaque DDoS ou attaque en déni de service est « une attaque destinée à interdire aux utilisateurs légitimes d'un service Internet de l'utiliser, en perturbant son fonctionnement et pouvant conduire à son blocage. Elle consiste à cibler un serveur, une adresse mail et à l'inonder de requêtes ou de mails. Imaginons des milliers de lettres que l'on essaie de faire entrer de force dans une boîte aux lettres individuelle placée dans l'entrée d'un immeuble : la boîte sature, la cage d'escalier est inondée de courrier, l'entrée de l'immeuble est bloquée. L'attaque peut être provoquée d'un poste, par un seul individu (attaque dite DOS pour *Deny of Service*) ou en mettant en œuvre un réseau d'ordinateurs robots, dit zombies, à travers un *botnet*, terme dérivé de *robot-network*. On parle alors d'attaque DDOS pour *Distributed Denial Of Service* ou « déni de service distribué ». Ce type d'attaque est très difficile à contrer. L'attaque DOS, par contre, peut se régler plus facilement, en inscrivant en site indésirable sur son pare-feu l'adresse IP d'origine de l'attaque »



Editée par

L'Institut du droit d'expression et d'inspiration françaises

Regard, Mai 2020

l'attribution d'une cyberattaque. En effet, à quel moment peut-on considérer qu'une attaque provient d'un Etat et comment le prouver conformément au droit international ? S'il est évident qu'aujourd'hui, le cyberspace n'est pas un Far-west où tout est permis car étant soumis à l'application du droit international²¹, l'attribution d'une cyberattaque est a priori une question technique. L'équation est encore plus difficile à résoudre quand on connaît les manœuvres des Etats en la matière qui se cachent derrière des acteurs privés (les proxies) pour perpétrer des attaques²². Certes d'autres principes de droit international aident dans l'attribution d'une cyberattaque comme le principe de « due diligence »²³. Sur ce principe, Karine BANNELIER affirme : « *le principe de cyber-diligence est intéressant car il permet d'engager la responsabilité d'un État et de réagir contre celui-ci à partir du moment où on prouve que l'attaque a été lancée ou a transité depuis les infrastructures de cet État et que celui-ci, alors qu'il savait et pouvait agir, n'a pris aucune mesure à sa disposition pour la prévenir ou l'arrêter, sans qu'il soit donc nécessaire de démontrer que l'État lui-même a dirigé ou contrôlé l'attaque* »²⁴. Remarquons toutefois qu'en pratique, les attributions répondent généralement à des considérations politiques.

Le risque de tensions entre les Etats est encore plus probable lorsque ces cyberattaques visent des infrastructures hospitalières dans une période de crise sanitaire. Malheureusement, de la France²⁵ en République Tchèque²⁶ en passant par la Lituanie²⁷, les exemples de ce type sur

²¹ « *Le droit international et, en particulier, la charte des Nations Unies sont applicables et essentiels au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement informatique ouvert, sûr, pacifique et accessible* » AGNU, 22 Juillet 2015, Res A/70/174, Groupe d'experts gouvernementaux sur les développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale, §24

²² Sur ces questions, voir Karine BANNELIER et Théodore CHRISTAKIS, *Cyberattaques- Préventions-réactions : rôle des Etats et des acteurs privés*, Les cahiers de la Revue Défense Nationale, Paris, 2017

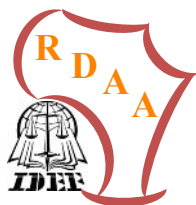
²³ Karine BANNELIER, *Obligations de diligence dans le cyberspace, qui a peur de la cyber-diligence*, Revue belge de droit international, 2017/2, Editions Bruylant, Bruxelles

²⁴ Karine BANNELIER-CHRISTAKIS, *Les cyberattaques toujours plus puissantes ...*, op.cit

²⁵ *L'assistance publique des hopitaux de Paris (AP-HP) a été la cible d'une attaque informatique nécessitant de couper, momentanément, l'accès externe aux mails et à des outils de télétravail*, [https://lexpansion-lexpress.fr/cdn.ampproject.org/c/s/lexpansion.lexpress.fr/high-tech/en-pleine-crise-du-coronavirus-les-hopitaux-de-paris-victimes-d-une-cyberattaque_2121692.amp.html]

²⁶ L'hôpital universitaire tchèque de Brno est également victime d'une cyberattaque ayant entraîné le report des interventions chirurgicales les plus urgentes et un transfert de patients vers un autre établissement de santé [<https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/>]

²⁷ Le ministère de la défense lituanienne a été la cible d'une cyberattaque. Leur adresse mail a été piratée et a permis aux attaquants d'envoyer des mails avec pour l'OTAN au nom de la Lituanie . [<https://www.lrt.lt/en/news-in-english/19/1153504/coronavirus-linked-cyber-attack-targets-lithuanian-defence-minister#>]



Regard, Mai 2020

des hôpitaux peuvent être multipliés. A cet égard, on peut dire que le COVID-19 n'infecte pas que les Hommes. Il pourrait bien affecter les relations internationales tout comme il impacte la protection des données personnelles.

II. L'incidence du COVID-19 sur la protection des données personnelles

Les activités humaines dans le cyberspace font générer des données personnelles en masse et leurs enjeux ont poussé à mettre un accent particulier sur leur protection. L'Union européenne a ainsi adopté le RGPD qui organise leur protection. Le COVID-19 occasionne cependant une collecte massive de données personnelles par des moyens diversifiés (A) dont le traitement s'avère exceptionnel à cause de l'urgence sanitaire (B).

A. Les augures d'une collecte massive de données personnelles par des moyens diversifiés

Pour faire face au COVID-19, les Etats recueillent des données de santé de leur population et pour s'assurer que les mesures de confinement prises sont respectées, certains Etats ont recueilli des données massives de géolocalisations ou sont tentés de le faire. Par exemple, la Chine a utilisé un système de « QR code médical »²⁸ que les populations sont obligées de montrer à la police avant de circuler dans plusieurs villes. Si, pour le gouvernement chinois, ce QR code permet d'évaluer le risque qu'une personne soit porteuse du coronavirus Covid-19, il présente des inquiétudes en ce que les données sont transmises à la police et viendraient conforter le système de crédit social déjà fonctionnel en Chine permettant aux autorités de passer au peigne fin les comportements des citoyens. Ces mesures éprouvent vraiment les limites de la vie privée.

En France, des questions se sont posées sur les possibilités de géolocalisation de la population. Les inquiétudes sur ces questions ont surtout été nourries par les SMS que le gouvernement a envoyés aux citoyens sur le COVID-19. Le gouvernement français collecterait-il les données à caractère personnel à des fins de géolocalisation et de traçage de la population ?

Il faut lever le doute et la CNIL²⁹ rassure en ce qui concerne les SMS reçus par les Français à

²⁸ MOZUR (P.), ZHONG (R.), KROLIK (A.), In coronavirus fight, China gives citizens and a color code, with red cards, The New York Times, 01/03/2020, consulté le 25/03/2020
[<https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html?referringSource=articleShare>]

²⁹ Commission nationale de l'informatique et libertés



Editée par

L'Institut du droit d'expression et d'inspiration françaises

Regard, Mai 2020

propos des consignes de sécurité à appliquer contre la propagation du COVID-19 : « Ce type d'opérations d'information est prévu par la loi qui impose aux opérateurs de télécommunications de diffuser, à leurs abonnés, les messages des pouvoirs publics destinés à prévenir la population d'un danger imminent ou d'une catastrophe majeure (article L. 33-1 du code des postes et des communications électroniques). Dans le cadre de cette opération, aucun numéro de téléphone n'a donc été transmis au gouvernement : celui-ci s'est contenté de transmettre un message aux opérateurs, qui se sont chargés, avec leurs propres bases de données, de l'acheminer vers les particuliers »³⁰.

Pourtant, les tentatives n'ont pas manqué en France. Les députés de l'opposition MM. CHAIZE et RETAILLEAU ont proposé l'amendement suivant dans le projet de loi d'urgence sanitaire : « Afin de faire face aux conséquences de l'épidémie de Covid-19 et en particulier d'assurer la continuité du fonctionnement des services et des réseaux mentionnés à l'article L. 732-1 du code de la sécurité intérieure, toute mesure visant à permettre la collecte et le traitement de données de santé et de localisation, est autorisée pendant une durée de six mois suivant la date de publication de la présente loi. »³¹ Selon eux, « Cet amendement vise à faciliter les procédures imposées aux opérateurs dans la collecte et le traitement des données de santé et de localisation. »³². L'amendement a été rejeté en première lecture mais le gouvernement dispose d'autres moyens légaux lui permettant de faire une collecte massive de données. La Quadrature du net en a fait une étude détaillée. Selon l'association, c'est la Loi de renseignement de 2015 qui en autoriserait le gouvernement si « les intérêts économiques majeurs »³³ de la France sont menacés. Or le COVID-19 n'est pas sans inquiéter l'économie nationale et nationale. Le président Macron l'a reconnu quand il a affirmé que « cette crise sanitaire sans précédent aura des conséquences [...] économiques majeures »³⁴.

Toutes ces dispositions sur fond du COVID-19 augurent une collecte massive de données personnelles³⁵ et le débat est loin d'être clos. Pour autant, faut-il s'inquiéter de la collecte des

³⁰ CNIL, *Le gouvernement s'adresse aux Français par SMS : le cadre légal applicable*, le 19 Mars 2020

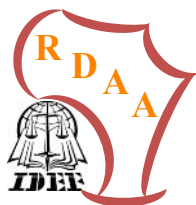
³¹ Projet de loi Faire face à l'épidémie de Covid-19 – P.J.L., amendement présenté par MM. CHAIZE et RETAILLEAU

³² Ibid

³³ Article L811-3 du code de la sécurité intérieure

³⁴ Emmanuel Macron, discours du 16 Mars 2020, *op cit*

³⁵ Sur ces questions, voir La quadrature du net, *Contre le COVID-19, la géolocalisation déjà autorisée*, 19/03/2020 consulté le 25/03/2020 [<https://www.laquadrature.net/2020/03/19/contre-le-covid-19-la-geolocalisation-deja-autorisee/>]



Regard, Mai 2020

données dans le cadre de la lutte contre le COVID-19 en France ?

B. Le traitement exceptionnel des données personnelles en France

Les bruits courent sur les intentions du gouvernement français d'utiliser les données personnelles afin de « mieux suivre la propagation de l'épidémie, en analysant les mouvements de population et donc les contaminations potentielles, et s'appuyer sur la localisation des smartphones pour faire respecter les obligations de confinement »³⁶. La commission européenne a, pour sa part, demandé aux opérateurs téléphoniques des données statistiques agrégées et non nominatives pour vérifier « si les consignes de confinement sont appliquées » et combattre la pandémie. Ces mesures nourrissent des inquiétudes mais que prévoit la loi ?

Il faut en effet se référer au RGPD qui dispose en son article 9 que le traitement des données à caractère personnel qui permettent « d'identifier une personne physique de manière unique » est interdit. Or les données de géolocalisation sont de nature à permettre ce type d'identification et tombent sous le coup de cette interdiction légale. Le principe n'est cependant pas absolu. Il comporte des exceptions parmi lesquelles deux retiennent particulièrement l'attention à l'heure du COVID-19. Il s'agit de l'exception tenant à la nécessité du traitement aux fins de « médecine préventive »³⁷ et celle tenant à la nécessité du traitement « pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé... sur la base du droit de l'Union ou du droit d'un Etat membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel »³⁸. Le traitement des données sensibles est donc autorisé s'il est fait dans ce cadre légal. Si on se réfère à la demande de la commission européenne et vu la menace que constitue la pandémie du COVID-19, les données agrégées et donc anonymisées ne violent pas ces dispositions du RGPD.

Enfin, le traitement des données sensibles est possible si la personne concernée donne son consentement. Aussi, tout projet de traçage numérique ne serait ni contraire à la loi ni attentatoire aux libertés fondamentales si son utilisation laisse aux citoyens la possibilité de donner clairement leur consentement.

La question du traitement des données de la santé a toujours suscité un débat houleux et engendré de grands contentieux entre le Gouvernement français et les représentants de la société

³⁶ TRUJILLO (E.), *Confinement: le gouvernement a-t-il le droit de récolter les données de nos smartphones?*, le 25/03/2020 consulté le 26/03/2020, [<https://www.bfmtv.com/tech/confinement-le-gouvernement-a-t-il-le-droit-de-recolter-les-donnees-de-nos-smartphones-1881933.html>]]

³⁷ RGPD, article 9 § h

³⁸ RGPD, article 9 § i



Regard, Mai 2020

civile³⁹. Il en a été ainsi du fichier SIVIC⁴⁰ établi à la suite des attentats de Paris de 2015 dans le but d'identifier et de compter les victimes et de faciliter la recherche des personnes portées disparues.⁴¹

Il faut cependant se garder de toute conclusion hâtive en ce qui concerne les stratégies numériques du gouvernement français dans la lutte contre le COVID-19, un débat devant être ouvert au parlement à ce propos pour fixer les garde-fous nécessaires pour préserver la démocratie et les libertés fondamentales.

Quoi qu'il en soit, les autorités de contrôle de la protection des données en Europe (CEPD) et en France (CNIL) passeront au peigne fin toutes les dispositions prises par les différentes institutions afin de sanctionner une éventuelle violation des droits et libertés.

Note biographique



KOUMAKO Yao Justin est Juriste Internationaliste se spécialisant en cybersécurité.

M. KOUMAKO a réalisé plusieurs études en la matière. Il a notamment étudié :

- « l'extraterritorialité du Cloud Act »
- « cybersécurité et protection des données personnelles dans le RGPD et dans la convention de Malabo »
- « la transformation numérique pour l'Afrique : réflexions sur les défis de sécurité et perspectives juridiques »
- « la problématique du déploiement de la technologie 5G en Afrique au regard de la défiance quasi-générale des états occidentaux »

Il prépare une thèse de doctorat en Droit international-Université Paris 2 Panthéon Assas sur le thème : « L'Etat à l'épreuve du cyberspace ».

³⁹ Voir FERAL-SCHUHL (C.), *La protection des données personnelles*, DALLOZ, 2019, p.19

⁴⁰ Système d'information pour le suivi des victimes

⁴¹ A ce propos, voir la délibération n°20166208 du 7 Juillet 2016 ainsi que les débats qui ont suivi l'autorisation du « SIVIC »



REVUE DU DROIT DES AFFAIRES EN AFRIQUE (RDAA)

Editée par

L'Institut du droit d'expression et d'inspiration françaises

Regard, Mai 2020

La Revue du Droit des Affaires en Afrique est publiée grâce au soutien de :



**Baker
McKenzie.**