n°27 Février 2021
#27 February 2021

# Lexing Insights

*Le réseau Lexing® vous informe – The Lexing® network informs you*

# GOUVERNANCE DE L'INTELLIGENCE ARTIFICIELLE
# GOVERNANCE OF ARTIFICIAL INTELLIGENCE

## REPONDRE AUX OPPORTUNITES ET AUX DEFIS JURIDIQUES POSES PAR L'IA

- 2021 va être une année particulièrement riche en actualités dans le domaine de l'IA : en vue de préparer la proposition législative de la Commission européenne sur le sujet, attendue en ce début d'année, le Parlement européen vient d'adopter un rapport contenant des lignes directrices pour les usages militaires et non militaires de l'IA, s'inscrivant dans le prolongement des trois résolutions adoptées fin 2020. Au même moment, entrera en vigueur la première norme internationale contraignante élaborée sous l'égide de l'ONU sur l'automatisation des véhicules de niveau 3 : les voitures volantes et autonomes, ce n'est plus de la fiction !
- Comme souligné par le réseau Lexing® lors de sa conférence consacrée à « l'IA et le droit », l'IA joue un rôle majeur dans la transformation numérique de nos sociétés. Notre vie quotidienne est de plus en plus gouvernée par les algorithmes : travail, santé, justice, police, transports, données personnelles…
- Quelles sont les différentes applications sectorielles de l'IA ? Comment sont-elles encadrées juridiquement ? Comment les différents pays du monde travaillent-ils à la gouvernance de l'IA afin de la réglementer au mieux et stimuler l'innovation tout en instaurant la confiance des citoyens ?
- Les membres du réseau Lexing® dressent un tableau de la situation actuelle à travers le monde. Les pays suivants ont contribué à ce numéro : Afrique du Sud, Belgique, Espagne, France, Grèce, Inde, Italie.

## HOW TO ADDRESS OPPORTUNITIES AND LEGAL CHALLENGES POSED BY AI

- *2021 is going to be a particularly busy year in the field of AI: to prepare the Commission's legislative proposal on this subject, expected at the beginning of the year, the European Parliament has just adopted a report containing guidelines for military and non-military use of AI, building on the three resolutions adopted at the end of 2020. The first binding international regulation on level 3 vehicle automation, developed under the aegis of the UN, will enter into force early 2021: flying and autonomous cars are no longer fiction!*
- *As pointed out by the Lexing network ® during its conference on "AI & Law", AI is a major part of the digital transformation. Our daily life is increasingly governed by algorithms: work, health, justice, police, transports, personal data…*
- *What are the different sectoral applications of AI? How are the multiple sectoral applications of AI regulated by law? How are different countries around the world working on AI governance to best regulate AI in order to boost innovation while building public trust?*

*The Lexing® network members provide a snapshot of the current state of play worldwide. The following countries have contributed to this issue: Belgium, France, Greece, India, Italy, Spain, South Africa.*

### *Lexing®*

Lexing® est le premier réseau international d'avocats en droit du numérique et des technologies avancées. Créé sur une initiative d'Alain Bensoussan, Lexing® permet aux entreprises internationales de bénéficier de l'assistance d'avocats alliant la connaissance des technologies, des métiers et du droit qui leur sont applicables dans leurs pays respectifs.

*Lexing® is the first international lawyers' network for digital and emerging law. Created on an initiative of Alain Bensoussan, Lexing® allows multinationals to benefit from the assistance of seasoned lawyers worldwide who each combines unique expertise in technology and industry with a thorough knowledge of law in their respective country.*

https://lexing.network

JEREMY BENSOUSSAN
*Directeur du département*
*Droit de l'IA et des technologies robotiques*
*du cabinet Lexing Alain Bensoussan-Avocats*

*Head of the AI & Robotics department*
*of Lexing Alain Bensoussan-Avocats*

## Vers un droit de l'intelligence artificielle en Afrique

▪ Le continent africain a aujourd'hui l'occasion unique de jouer un rôle pionnier dans la règlementation de l'IA en adoptant une approche éthique, fondée sur des principes, qui guidera les pays qui le compose pendant les décennies à venir. L'Afrique doit saisir cette opportunité sous peine d'être à la traîne du reste de la communauté mondiale en matière d'l'IA.

### L'IA aura une incidence considérable pour l'humanité

▪ Omniprésente, l'IA est présentée comme une technologie qui va radicalement changer le monde. Selon les experts, elle va révolutionner l'ensemble des secteurs d'activité et représenter un bouleversement aussi important que l'avènement de l'électricité. Une chose est sûre, l'IA aura une incidence considérable pour l'humanité.

▪ Cette incidence peut être positive, mais aussi négative. En effet, l'IA a déjà été à l'origine d'actions ou des décisions néfastes pour l'être humain. Par exemple, une IA entraînée avec des données contenant des préjugés raciaux ou sexistes a ensuite pris des mesures discriminatoires à l'égard de certains groupes de personnes. C'est pourquoi d'aucuns appellent de leurs vœux un encadrement juridique de l'IA.

### Nous avons besoin d'une réglementation pour protéger l'humanité

▪ Certains pays ont d'ores et déjà entamé un processus de réglementation. En Afrique du Sud, le gouvernement a créé la commission présidentielle sur la quatrième révolution industrielle. Cette commission est chargée d'évaluer les avantages de l'IA pour le pays et de conseiller les organismes de réglementation sur les lois relatives à l'IA. Le Kenya et la Tanzanie ont également adopté une politique de régulation de l'IA.

▪ De son côté, l'Union européenne a posé d'importants jalons en matière de réglementation des robots. En outre, certaines régions du monde ont choisi de légiférer dans le même temps dans le domaine de la protection de la vie privée. C'est le cas par exemple l'UE avec le RGPD, et l'Afrique du Sud avec la loi n°4 de 2013 sur la protection des informations personnelles (POPIA), qui encadrent tous deux la prise de décision automatisée.

▪ L'objectif des législateurs étant de protéger les êtres humains et l'IA fonctionnant au-delà des frontières des pays, il serait préférable que les lois qui régissent l'IA s'appliquent partout de manière uniforme.

▪ L'Afrique s'emploie à devenir une société à forte orientation technologique. Si certains pays africains ont adopté une politique sur la manière dont ils devraient réglementer l'IA, le risque est que ces différentes réglementations manquent de

cohérence. Quelles mesures pourraient donc prendre l'Afrique pour adopter une approche uniforme de la réglementation de l'IA ?

### Première étape : créer une commission africaine sur l'IA

▪ L'Afrique doit se doter d'une commission centrale qui dirigera l'action de l'ensemble du continent dans le domaine de l'IA. Cette commission aurait pour mission d'étudier les aspects éthiques, juridiques et socio-économiques de l'IA. L'intérêt des citoyens africains doivent être au cœur des préoccupations dans ce domaine. De plus, cette commission doit œuvrer à promouvoir le rôle de l'Afrique pour en faire un concurrent clé sur le marché mondial de l'IA.

▪ Cette autorité pourrait être composée d'experts dans les domaines du droit et des technologies, l'idéal étant naturellement de rassembler des personnes avec des profils à double compétences, combinant des connaissances juridiques et techniques. Les membres de la commission devraient être issus de tous des pays africains, de manière à ce que chaque pays soit représenté.

▪ Parmi les nombreuses responsabilités de cet organisme figurerait l'élaboration de principes pour guider les nations africaines dans la création d'une politique d'IA et la mise en place d'une réglementation de l'IA. Ces principes doivent jeter les bases d'une IA digne de confiance pour les citoyens africains.

▪ En élaborant les principes africains en matière d'IA, la commission devrait s'inspirer des travaux déjà réalisés à l'international et tirer des enseignements des approches suivies par d'autres pays, tout en tenant dument compte de la jurisprudence constitutionnelle africaine. A cet égard, les principes de Johannesburg relatifs à la sécurité nationale constituent un précédent éclairant, bien que dans un domaine d'application différent.

### Prochaine étape : identifier l'approche à appliquer pour réglementer l'IA

▪ Plusieurs pays s'interrogent sur la manière de règlementer l'IA, qui est une technologie sophistiquée et évolutive, sachant qu'Il est nécessaire de trouver un équilibre entre les droits de l'homme et le progrès technologique.

▪ La meilleure approche pour réglementer l'IA est d'adopter une réglementation fondée sur des principes et formulée en termes simples, l'idée étant d'établir un petit nombre de lois en langage clair, que les citoyens puissent comprendre, connaitre, et ainsi respecter. De fait, en l'espèce, les réglementations fondées sur des règles ne sont pas appropriées car elles entraveraient les avancées de l'IA. La loi POPIA adoptée en Afrique du Sud est, notamment, un bon exemple de législation fondée sur des principes.

JOHN GILES

south-africa@lexing.network

*Towards a law of artificial intelligence for Africa*

▪ *Africa has a unique opportunity to pioneer an ethical and principle-based approach to regulating AI that will guide its nations for decades to come. It's time for it to seize this opportunity to avoid the risk of being left behind in the global AI community.*

*AI will have a significant impact on humanity*

▪ *Globally, AI is ubiquitous. The picture that's painted is of a technology that will fundamentally change the world. Leading experts say it will disrupt almost every imaginable industry. Other experts even call it the next best thing after "electricity". What's evident is that AI will likely have a significant impact on humanity.*

▪ *The impact will be good, but it could also be harmful. There are several instances where AI has already performed actions or made decisions that don't benefit humanity. For example, AI trained on datasets containing racial or gender bias has unfairly discriminated against certain groups of people. Hence, there's been a call for regulation.*

*We need regulation to protect humanity*

▪ *Some countries have started the process of regulation. In South Africa, the government has established the President's Commission on the Fourth Industrial Revolution. The Commission will investigate how AI will benefit the country and advise regulatory bodies on AI laws. Both Kenya and Tanzania have also adopted policy about the regulation of AI.*

▪ *The EU has already made significant progress on regulating robots. Further, there are regions which have elected to legislate also within a privacy context, e.g. the EU's GDPR and South Africa's Protection of Personal Information Act 4 of 2013 (or POPIA) regulates automated decision-making.*

▪ *The intention behind the regulation is to protect humanity. However, AI will probably work across many jurisdictions. So, it would be better if the laws that regulate AI apply uniformly.*

▪ *Africa has been working steadily towards becoming a technology-driven society. Some African countries have also adopted a policy on how they should regulate AI. However, the risk is that the regulation could be haphazard. This article explores how Africa can adopt a uniform approach to the regulation of AI.*

*The start - an African commission on AI*

▪ *We need a central commission that will lead Africa in dealing with AI. It should focus on the ethical, legal, and socio-economic aspects of AI. In dealing with AI, African citizens need to be at the centre of the considerations. Moreover, the Commission should consider Africa's role as a key competitor in the global AI market.*

▪ *The body must consist of the best minds in law and technology; the prize would be dually qualified individuals. Further, the members of the Commission should be representatives from each African country.*

▪ *Among the several general responsibilities of this body, it must develop principles to guide African nations in creating AI policy and regulating AI. The principles should lay the foundation for good AI that builds trust with African citizens.*

▪ *In thoughtfully producing the African AI principles, the Commission should consider international lessons from other jurisdictions. However, it must ground the lessons in African constitutional jurisprudence. A good example of similar principles, albeit within national security, are the Johannesburg Principles.*

*Next – how should nations regulate AI?*

▪ *Several nations are grappling with how to regulate AI. The reason is that it's an advanced and dynamic technology. There's a need to balance human rights against technological advancement.*

▪ *The best approach to regulating AI is principle-based regulation couched in simple law (a few laws in plain language that people understand and know, and then comply with). Rules-based regulations are inappropriate because they will prevent AI from advancing in meaningful ways. An excellent example of principle-based legislation is South Africa's POPIA.*

JOHN GILES

south-africa@lexing.network

## Open data, justice prédictive et IA en Belgique

### La loi du 5 mai 2019 : point de départ de l'avènement de l'IA dans la justice belge ?

▪ Cette loi **(1)**, publiée au Moniteur belge le 16 mai 2019 et entrée en vigueur le 1er septembre 2020, impose la publication, en ligne, dans une base de données accessible à tous les citoyens, de tous les arrêts et jugements prononcés par les juridictions belges. Elle concrétise ainsi, dans l'environnement numérique, le prescrit de l'article 149 de la Constitution **(2)** et laisse présager l'avènement de l'analyse des décisions judiciaires par des outils d'intelligence artificielle.

### L'apanage des – grandes – entreprises privées

▪ Pour des raisons liées au respect de la vie privée des justiciables, les décisions doivent être anonymisées. Vu les ressources technologiques à disposition du Ministère de la Justice (SPF Justice), ce sont de grandes entreprises du secteur privé qui se chargeront (et qui se chargent déjà) du processus, d'une part, d'anonymisation des coordonnées des parties et des magistrats et d'autre part, de la publication de celles-ci. Par ailleurs, de nombreuses startups sont déjà sur le pont pour surfer sur la vague de « *l'ubérisation* » de la justice.

### Anonymisation et publication

Les modalités pratiques pour y parvenir ne sont pas encore établies mais des grandes entreprises d'éditeurs juridiques s'occupent déjà de fournir les bases de données en ligne de décisions anonymisées. Agissant en tant que responsable du traitement, responsable conjoint ou sous-traitant pour le SPF Justice (ces précisions sont encore à déterminer), ces dernières doivent en tout état de cause assurer le respect des garanties de sécurité des données et d'information des citoyens telles que prévues par le RGPD **(3)**, avant de rendre ces données à caractère personnel anonymes.

### Utilisation par les cabinets d'avocats et les « legaltechs »

▪ Sans parler de « juges-robots », l'existence d'une banque de données regroupant toutes les décisions judiciaires permet l'utilisation de l'intelligence artificielle pour, d'une part, traiter de façon automatisée les litiges dont l'enjeu n'est pas élevé et, d'autre part, aider les avocats dans leur rôle de conseil de leurs clients, via l'aide à la recherche juridique par exemple. Ainsi, de grands cabinets d'affaires internationaux bruxellois ont déjà recours à des outils de recherches mus par l'intelligence artificielle dans le cadre de dossiers de *due diligence*.

▪ Néanmoins, il convient, pour les cabinets d'avocats, de prendre garde lorsqu'ils recourent aux systèmes intelligents dans le cadre de leur mission de conseil. En

REFERENCES

(1) Loi modifiant le Code d'instruction criminelle et le Code judiciaire en ce qui concerne la publication des jugements et des arrêts

(2) Constitution belge

(3) Règlement général sur la protection des données, 2016/67.

Code de droit économique, 28 février 2013

effet, il se pourrait qu'un client, ayant été débouté, se retourne contre son avocat, au motif que ce-dernier :

- soit, ait suivi « aveuglément » les résultats offerts par l'outil d'intelligence artificielle, sans avoir porté un regard personnel critique sur ceux-ci ;

- soit, n'ait pas suivi les résultats offerts par cet outil intelligent et par ce fait, compromis l'issue du litige à l'égard du client.

▪ Dès lors, il peut être utile pour l'avocat de (déjà) préciser, dans ses conditions générales, qu'il a recours à des outils informatiques intelligents (devoir d'information de l'avocat à l'égard de son client) dans le cadre de sa mission de conseil, en précisant que cet usage n'est réalisé qu'à titre purement informatif et rappeler ainsi qu'il n'est tenu qu'à une obligation de moyen. Ainsi, l'avocat s'assurerait de s'exonérer de toute responsabilité quant à l'issue du litige. Il en irait de même pour les nombreuses « *legaltechs* » florissantes sur le marché du conseil juridique.

JOACHIM
PARMENTIER

belgium@
lexing.network

REFERENCES

*Open data, predictive justice and AI in Belgium*

## *The Act of May 5th, 2019: starting point in the advent of AI in the Belgian justice system?*

▪ *This Act, published in the Belgian Official Journal ("Moniteur belge") on May 16th, 2019 and that came into force on September 1st, 2020, requires the online publication, in a database accessible to all citizens, of all judgments handed down by Belgian courts. It thus gives concrete expression in the digital environment to the Article 149 of the Constitution and foreshadows the advent of the analysis of judicial decisions by artificial intelligence tools.*

## *The privilege of - large - private companies*

▪ *For reasons related to the respect of the private life of individuals, decisions must be anonymized. Given the technological resources available to the Ministry of Justice (FPS Justice), it is large private sector companies that will (and already do) the process of anonymizing the personal data of the parties and magistrates, on the one hand, and publishing them, on the other. In addition, many startups are already on deck to ride the wave of the "uberization" of justice.*

## *Anonymization and publication*

▪ *The practical modalities for doing so are not yet established, but major legal publishing companies are already working to provide online databases of anonymized decisions. Acting as data controllers, joint controllers or processors for the FPS Justice (these details are yet to be determined), these companies must in any case ensure compliance with the guarantees of data security and information of citizens as provided for by the GDPR, before making these personal data anonymous.*

## *Use by law firms and legaltechs*

▪ *Without speaking of "robot judges," the existence of a database of all judicial decisions allows the use of artificial intelligence to, on the one hand, automatically process litigation where the stakes are not high and, on the other hand, help lawyers in their role of advising their clients, through legal research assistance for example. For instance, major international business law firms in Brussels already use artificial intelligence-driven search tools in the context of due diligence cases.*

▪ *Nevertheless, law firms should be cautious when using intelligent systems as part of their consulting mission. Indeed, one can imagine that a client, who lost a case, could turn against his lawyer, on the grounds that the latter:*

(1) *Act amending the Code of Criminal Procedure and the Judicial Code with respect to the publication of judgments and rulings*v.

*(3) Belgian Constitution*

*(2) General Data Protection Regulation, 2016/67.*

*Code of economic law, February 28th, 2013*

- *either, has "blindly" followed the results offered by the artificial intelligence tool, without having taken a critical personal look at them;*

- *or, did not follow the results offered by this intelligent tool and, by this fact, compromised the outcome of the client's case.*

▪ *Consequently, it may be useful for the law firm to (already) specify, in its general terms and conditions, that it uses intelligent computer tools (the lawyer's duty to inform his client) in the context of his mission as counsel, specifying that this use is purely for information purpose and thus reminding that he is only bound by an obligation of means. In this way, the law firm would ensure that it is not liable for the outcome of the litigation. The same would apply to the many "legaltechs" flourishing on the legal advice market.*

JOACHIM
PARMENTIER

belgium@
lexing.network

## IA et secteur public

▪ En avril 2018, la Commission européenne a adopté sa première stratégie d'AI, axée sur l'augmentation des investissements, la multiplication des données disponibles, la promotion des talents et la garantie de la confiance.

▪ Toutefois, le niveau de mise en œuvre de l'IA dans le secteur public en Espagne est loin de l'utilisation maximale de ce type de technologie, un fait qui est très pertinent à un moment où l'utilisation de l'IA pourrait contribuer à atténuer les effets de la pandémie.

▪ Parmi les principaux défis à relever figure la nécessité de maintenir les services de base pleinement opérationnels, malgré les mesures de sécurité mises en place, telles que la distanciation sociale. De même, la nouvelle réalité du télétravail implique également la nécessité d'une adaptation pour de nombreux fonctionnaires et citoyens ordinaires.

▪ Par exemple, le département de l'emploi, de la formation et du travail indépendant du gouvernement régional d'Andalousie a récemment déployé une solution d'intelligence artificielle pour aider des milliers de travailleurs indépendants qui ont demandé des subventions d'urgence. Développée en deux semaines, cette solution a permis de réduire de deux mois le délai de résolution des subventions pour 150 000 demandeurs et a libéré de manière significative 20 000 employés, leur permettant d'apporter une plus grande valeur à leur mission d'aide à un plus grand nombre de citoyens.

▪ Parmi les aspects les plus importants de la mise en œuvre de la IA dans le secteur public, nous pouvons souligner les suivants :

### La nécessité de donner la priorité à l'IA aux plus hauts niveaux de direction

▪ L'IA offre aux organisations la possibilité de bénéficier de processus opérationnels améliorés, car les outils comportant des éléments d'IA peuvent aider à gérer des tâches simples ou répétitives. Toutefois, la principale valeur vient de son utilisation pour innover et renforcer les services et expériences clés, et lorsqu'il est destiné à soutenir les personnes plutôt qu'à les remplacer.

▪ Par exemple, dans le cadre de la modernisation de la justice en Espagne, afin d'être à l'avant-garde des nouvelles technologies, notamment l'AI, l'Association des bureaux d'enregistrement (Colegio de Registradores) a créé il y a deux ans un comité de l'innovation dont l'objectif est d'analyser les technologies émergentes sur le marché et la manière dont elles peuvent être intégrées à l'organisation. Le comité se concentre également sur la mise en œuvre de nouvelles solutions avec prudence pour éviter les risques.

## L'importance de l'équité et de la transparence des algorithmes

▪ Par exemple, un hôpital pourrait utiliser l'IA pour concevoir un plan de traitement personnalisé pour un patient, tandis qu'une agence gouvernementale pourrait l'utiliser pour identifier les citoyens à risque d'exclusion qui pourraient bénéficier d'un service social particulier. Il est impossible de mesurer l'importance de ce type de décisions. L'application équitable et éthique d'un algorithme est donc d'une importance vitale pour garantir que chacun soit traité équitablement. Pour toute organisation - qu'il s'agisse d'une administration publique, d'un hôpital ou d'un établissement d'enseignement - il est essentiel d'établir et de maintenir la confiance pour que les employés et les citoyens soient à l'aise avec l'utilisation de l'IA. Par conséquent, tous les postes concernés au sein d'une organisation doivent être formés pour comprendre leur obligation de traiter les données de manière éthique et responsable.

## La formation en IA

▪ Cependant, le plus important pour s'assurer que les organisations ont les compétences nécessaires dans l'utilisation de l'IA est de créer une culture de la formation qui ne se limite pas à dispenser des cours, mais qui inculque également la valeur de l'apprentissage comme moyen d'améliorer l'impact, la flexibilité et la réinvention.

MARC GALLARDO

spain
@lexing.network

*IA and Public Sector*

▪ *In April 2018, the European Commission adopted its first AI strategy, focused on increasing investment, increasing available data, fostering talent and ensuring trust.*

▪ *However, the level of AI implementation in the public sector in Spain is far from the maximum use of this type of technology, a fact that becomes highly relevant at a time when the use of AI could help mitigate the effects of the pandemic.*

▪ *Among the main challenges are the need to keep basic services fully operational, despite the security measures in place, such as social distancing. Similarly, the new reality of teleworking also implies the need for adaptation for many civil servants and ordinary citizens.*

▪ *For example, recently the Department of Employment, Training and Self-Employment of the Andalusian Regional Government deployed an Artificial Intelligence solution to help thousands of self-employed people who were claiming emergency subsidies. Developed in two weeks, this solution decreased the time to resolve the subsidies by two months for 150,000 applicants and considerably freed up 20,000 employees, allowing them to provide greater value in their mission to help more citizens.*

▪ *Among the most important aspects of the implementation of the IA in the Public Sector, we can highlight the following:*

*The need to prioritize AI at the highest levels of leadership*

▪ *AI offers organizations the opportunity to benefit from improved operational processes, as tools with AI components can help manage simple or repetitive tasks. However, the main value derives from using it to innovate and strengthen key services and experiences, and when it is intended to support people rather than replace them.*

▪ *For example, within the scope of the modernization of justice in Spain, in order to be at the forefront of new technologies, particularly AI, the Association of Registrars (Colegio de Registradores) created two years ago an innovation committee whose objective is to analyze emerging technologies in the market and how these can be incorporated into the organization. The committee also focuses on the application of new solutions with caution to avoid risks.*

*The importance of fairness and transparency of algorithms*

▪ *For example, a hospital might use AI to design a personalized treatment plan for a patient, while a government agency might use it to identify citizens at risk of*

*exclusion who could benefit from a particular social service. It is impossible to measure the importance of these types of decisions. The fair and ethical application of an algorithm is therefore of paramount importance to ensure that everyone is treated fairly. For any entity - be it a public administration, a hospital or an educational institution - building and maintaining trust is critical to ensure that both employees and citizens are comfortable with the use of Artificial Intelligence. Therefore, all relevant positions within an organization must be trained to understand their obligation to treat data ethically and responsibly.*

*Training on IA*

▪ *The most important thing, however, to ensure that organizations have the necessary skills in the use of AI is to create a training culture that is not just about delivering courses, but also instills the value of learning as a means to improve impact, flexibility and reinvention.*

MARC GALLARDO

spain
@lexing.network

## IA, police prédictive et reconnaissance faciale

- La reconnaissance faciale est mise en œuvre par l'Etat, en France, à des fins de :
  - contrôles douaniers, par le déploiement du passeport biométrique et du Système de passage automatisé rapide aux frontières extérieures (Parafe) ;
  - gestion de l'identité numérique régalienne, avec la mise en place du système d'authentification en ligne certifiée sur mobile (Alicem), récemment validée par le Conseil d'Etat **(1)** ;
  - sécurité, de surveillance et d'identification sur la voie publique de personnes recherchées.

- Dans le cadre de cette dernière finalité, de nombreux fichiers de police sont utilisés. Notamment, la reconnaissance faciale s'appuie sur les fichiers de traitement des antécédents judiciaires (TAJ) et de gestion automatisée des signalements et des photo anthropométriques répertoriées et distribuables (Gaspard), ce dernier fichier contenant les photographies saisies durant les enquêtes et prises lors des gardes à vue.

- Le nombre de fichier pouvant servir de support à l'emploi de la reconnaissance faciale est en constante augmentation. A titre d'illustration, le début de l'année 2020 a été marquée par l'autorisation de la mise en œuvre d'un traitement permettant la dématérialisation de la prise de notes par les militaires de la gendarmerie nationale **(2)**, et la fin de l'année 2020 par la publication de trois décrets venant modifier les traitements de renseignement territorial de la police **(3)** (PASP), de la gendarmerie **(4)** (GIPASP) et relatif aux enquêtes administratives **(5)**.

### Recours aux outils de police prédictive

- Les outils de police prédictive ont pour finalités d'anticiper la commission des infractions et d'assister les services enquêteurs dans leurs investigations.

- De nombreux logiciels, à l'instar de PredPol, HunchLab ou Palantir, sont développés par des sociétés commerciales, et permettent de réaliser un ciblage des lieux ou des individus dans la perspective de prévenir la commission d'infractions. Ces outils ne sont pas à l'heure actuelle employés par les services français.

- En France, la gendarmerie développe Paved, un outil de prévention des cambriolages et des dégradations de véhicules, qui, par l'analyse des données localisées des délits précédents, identifie les zones où ces infractions pourraient être commises. Il permet ainsi le déploiement d'unités sur le terrain, dans un but dissuasif.

- La gendarmerie a fait le choix de développer elle-même cet outil afin de « garder la main sur un logiciel créé en interne, avec des ingénieurs, programmeurs et data scientists gendarmes » **(6)**.

## REFERENCES

(1) Conseil d'Etat, 4-11-2020, N° 432656

(2) Décret n° 2020-151 du 20 février 2020 portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « application mobile de prise de notes » (GendNotes)

(3) Décret n° 2020-1511 du 2 décembre 2020 modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Prévention des atteintes à la sécurité publique »

(4) Décret n° 2020-1512 du 2 décembre 2020 modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Gestion de l'information et prévention des atteintes à la sécurité publique »

(5) Décret n° 2020-1510 du 2 décembre 2020 modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Enquêtes administratives liées à la sécurité publique »

(6) Céline Castets-Renard, Philippe Besse, Jean-Michel Loubes, Laurent Perrussel. Encadrement des risques techniques et juridiques des activités de police prédictive. [Rapport de recherche] Centre des Hautes Etudes du Ministère de l'Intérieur. 2019. ffhal-02190585

(7) Virginie Bensoussan-Brulé, AnaCrim, les logiciels d'analyse criminelle de la gendarmerie, 8-7-2017, https://www.alain-

▪ L'emploi de tels outils doit être mis en parallèle avec le recours à l'utilisation des outils d'analyse criminelle. Ces outils, au premier rang desquels figure le logiciel Anacrim, sont utilisés par les services enquêteurs français pour la résolution d'affaires complexes (7).

### Encadrement du recours aux outils de reconnaissance faciale et de police prédictive

▪ Le recours aux outils de reconnaissance faciale et de police prédictive suppose nécessairement le respect des droits fondamentaux.

▪ Dès 2008, le Sénat avait considéré que « les perspectives de développement de la biométrie, en particulier de la reconnaissance faciale, relèvent incontestablement de la Cnil » (8).

▪ Ainsi, les traitements des données personnelles à des fins de prévention et de détection des infractions pénales sont encadrés par les dispositions de la directive « Police-Justice » (9), transposée en France au sein du titre III de la loi Informatique et Libertés (10).

▪ Le recours aux outils d'analyse criminelle est en outre encadré par les dispositions d'un décret du 7 mai 2012 (11) qui prévoit notamment le cadre de leur utilisation, les personnes destinataires des données et informations et les règles de conservation des traces de consultation et d'utilisation.

▪ Dans une résolution du 20 octobre 2020, le Parlement européen est venu préciser que l'utilisation de la reconnaissance faciale « doit toujours être rendue publique et être proportionnée, ciblée, limitée à des objectifs spécifiques et limitée dans le temps dans le respect du droit de l'Union, et tenir dûment compte de la dignité et de l'autonomie humaines, ainsi que des droits fondamentaux énoncés dans la Charte », et faire l'objet d'un contrôle juridictionnel et d'une surveillance démocratique (12).

▪ Dans cette même résolution, le Parlement européen fait état de réserves quant au déploiement des technologies d'intelligence artificielle dans le cadre des activités de police, et cible spécifiquement le recours aux outils de police prédictive.

▪ Constatant qu'il « présente des avantages », le Parlement souligne toutefois qu'« il peut conduire à de graves abus, tels que la surveillance de masse, la police prédictive et les violations des droits de la défense ».

▪ Si le recours aux outils de police prédictive n'a pas fait à ce jour l'objet d'une décision judiciaire française, l'emploi de la reconnaissance faciale a récemment fait son entrée dans les tribunaux lorsque, le 31 octobre 2019, le Tribunal correctionnel de Lyon a, dans une affaire de vol, validé l'utilisation, par les gendarmes, d'un dispositif de reconnaissance faciale.

bensoussan.com/avocats/anacrim-logiciels-danalyse-criminelle/2017/07/18/

(8) Sénat, rapport d'information n°131, « La vidéosurveillance : pour un nouvel encadrement juridique », 10-12-2008

(9) Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données

(10) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

(11) Décret n° 2012-689 du 7 mai 2012 relatif aux conditions de mise en œuvre des fichiers d'analyse sérielle et des logiciels de rapprochement judiciaire

(12) Parlement européen, Résolution contenant des recommandations à la Commission concernant un cadre d'aspects éthiques en matière d'intelligence artificielle, de robotique et de technologies connexes (2020/2012(INL), 20-10-2020

RAPHAËL LIOTIER

france
@lexing.network



### *AI, predictive policing and facial recognition*

- *In France, facial recognition is used by the state for the purposes of:*
  - *enforcing customs controls, through the deployment of the biometric passport and the 'Parafe' eGates (automated fast track crossing at external borders);*
  - *managing digital identity, with the implementation of the certified online authentication system mobile app (Alicem), recently validated by the Council of State* ***(1)****;*
  - *ensuring security, surveillance and identification of wanted persons on the public highway.*

- *For the identification of wanted persons, numerous police files are used. In particular, facial recognition taps into the criminal records database (TAJ) and the anthropometric photographs database (GASPARD) that contains photographs seized during investigations and taken during police custody.*

- *The number of files that can be used to support facial recognition is constantly increasing. For example, the beginning of the year 2020 was marked by the authorization of the implementation of a process allowing the digitization of note-taking by the military of the gendarmerie nationale* ***(2)****, and the end of the year 2020 by the publication of three decrees modifying the processing of territorial intelligence by the police (PASP)* ***(3)*** *and the gendarmerie (GIPASP)* ***(4)*** *and relating to administrative investigations (EASP)* ***(5)****.*

### *Use of predictive policing tools*

- *Predictive policing tools aim to anticipate the commission of offences and to assist the investigation services in their tasks.*

- *Many software programs developed by commercial companies, such as PredPol, HunchLab or Palantir, enable to target places or individuals with a view to preventing the commission of offences. This type of tools is not currently used by French law enforcement agencies.*

- *In France, the gendarmerie is developing Paved, a tool to prevent burglary and car theft, which, by analyzing localized data from previous offences, identifies areas where these offences could be committed. Using Paved data, the gendarmerie can then deploy units in the identified hotspots for deterrence purposes.*

- *The gendarmerie has chosen to develop this tool itself in order to "keep control over software created in-house, with officers who are engineers, programmers and data scientists"* ***(6)****.*

*(1) Conseil d'Etat, 4-11-2020, N° 432656*

*(2) Decree no. 2020-151 of 20 February 2020 authorizing the automated processing of personal data known as "mobile note-taking application" (GendNotes)*

*(3) Decree No. 2020-1511 of 2 December 2020 amending the provisions of the Internal Security Code relating to the processing of personal data known as "Prevention of public security breaches".*

*(4) Decree No. 2020-1512 of 2December 2020 amending the provisions of the Internal Security Code relating to the processing of personal data known as "Information management and prevention of public security breaches".*

*(5) Decree No. 2020-1510 of 2 December 2020 amending the provisions of the Internal Security Code relating to the processing of personal data known as "Administrative investigations related to public security".*

*(6) Céline Castets-Renard, Philippe Besse, Jean-Michel Loubes, Laurent Perrussel. Encadrement des risques techniques et juridiques des activités de police prédictive. [Rapport de recherche] Centre des Hautes Etudes du Ministère de l'Intérieur. 2019. ffhal-02190585*

*(7) Virginie Bensoussan-Brulé, AnaCrim, les logiciels d'analyse criminelle de la gendarmerie, 8-7-2017, https://www.alain-bensoussan.com/avocats/anacrim-logiciels-danalyse-criminelle/2017/07/18/*

▪ *Along such tools, there are also criminal analysis tools. These tools, such as the Anacrim software, are used by the French investigation services for the resolution of complex cases* ***(7)****.*

*Regulating the use of facial recognition and predictive policing tools*

▪ *The use of facial recognition and predictive policing tools necessarily implies the respect of fundamental rights.*

▪ *In 2008, the Senate considered that "the prospects for the development of biometrics, in particular facial recognition, undeniably fall within the remit of the CNIL"* ***(8)****.*

▪ *The processing of personal data for the purposes of preventing and detecting criminal offences is governed by the provisions of the European Police and Criminal Justice Data Protection Directive* ***(9)****, implemented into French law under Title III of the Data Protection Act* ***(10)****.*

▪ *Criminal analysis tools are also governed by the provisions of a decree of 7 May 2012* ***(11)****, which provides in particular how they should be used, who could receive the related data and information and what rules should be followed for storing traces of their consultation and use.*

▪ *In a resolution dated 20 October 2020, the European Parliament specified that the use of facial recognition "should always be disclosed, proportionate, targeted and limited to specific objectives, restricted in time in accordance with Union law and have due regard for human dignity and autonomy and the fundamental rights set out in the Charter", and be subject to judicial review and democratic scrutiny* ***(12)****.*

▪ *In the same resolution, the European Parliament expressed reservations about the deployment of AI technologies in policing, and specifically targets the use of predictive policing tools.*

▪ *While noting that it "has benefits", the European Parliament also pointed out that "it can result in grave misuse, such as mass surveillance, predictive policing and breaches of due process rights".*

▪ *The use of predictive policing tools has not yet been the subject of a French court decision, but the use of facial recognition recently made its debut in the courts when, on 31 October 2019, the Lyon Criminal Court validated the use of a facial recognition device by the gendarmes in a theft case.*

*(8) Sénat, information report n°131, « La vidéosurveillance : pour un nouvel encadrement juridique [Video surveillance: for a new legal framework], 10-12-2008*

*(9) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by the competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data.*

*(10) Law No. 78-17 of 6 January 1978 on information technology, data files and civil liberties.*

*(11) Decree No. 2012-689 of 7 May 2012 relating to the conditions of implementation of serial analysis files and software for judicial reconciliation.*

*(12) European Parliament, Resolution with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL), 20-10-2020.*

RAPHAËL LIOTIER

france
@lexing.network

## Intelligence artificielle et ressources humaines

▪ Les technologies de l'IA sont omniprésentes dans notre quotidien, tant dans la sphère privée que dans la sphère professionnelle. Les applications commerciales de l'IA offrent en effet aux entreprises de réelles possibilités de développement et de restructuration de leur production. L'IA est notamment de plus en plus utilisée dans le secteur des ressources humaines (RH). Cependant, l'IA s'accompagne de certains risques juridiques, dont les dirigeants doivent être bien conscients avant de décider d'avoir recours à des outils et des applications d'IA au sein de leurs structures.

▪ D'un côté, la mise en œuvre des technologies d'IA dans le secteur des RH peut accroître l'efficacité (et potentiellement l'équité) des décisions prises au cours du procédure de recrutement, et également contribuer à l'amélioration des conditions de travail. D'un autre côté, les risques associés ne sont pas négligeables : notamment, l'opacité des algorithmes est problématique à l'heure où la transparence et la non-discrimination sont des obligations légales et des priorités éthiques pour les organisations.

▪ La gamme d'applications de l'IA dans le secteur des RH est vaste :

- l'IA peut, par exemple, identifier les meilleurs candidats pour certaines fonctions, apparier les exigences du poste et les compétences et l'expérience requises, recommander des emplois et des fonctions spécifiques aux candidats potentiels, etc. Les assistants RH numériques sont capables de filtrer un grand nombre de CV et de références, en dégageant des critères communs entre les candidats et les personnes ayant déjà effectué les mêmes tâches avec succès ;
- par ailleurs, les outils d'IA peuvent observer les réactions et l'attitude des candidats lors des entretiens et repérer et évaluer et analyser des éléments qu'un recruteur humain ne serait pas en mesure, du moins facilement, d'identifier et d'évaluer ;
- les outils d'IA peuvent analyser les données du marché et fournir des informations utiles sur les salaires, la durée du contrat, etc., contribuant ainsi à la réussite du recrutement et de la gestion de travailleurs clés (par exemple, en traduisant les données personnelles et comportementales en termes de productivité, d'efficacité et d'implication dans les tâches assignées).

▪ La mise en œuvre des technologies d'IA dans les RH se situe au carrefour du droit de la protection des données, du droit du travail et des réglementations de lutte contre la discrimination. Le « Livre blanc sur l'intelligence artificielle » de la Commission européenne définit l'approche de l'Union européenne en matière de technologies d'IA et souligne les risques potentiels de l'IA dans ce secteur. L'utilisation de l'IA à des fins de recrutement y est désignée comme étant « à haut

risque », nécessitant la mise en place d'exigences essentielles (par exemple, le contrôle humain) afin d'apporter des garanties spécifiques. En particulier, le traitement de catégories spéciales (sensibles) de données à caractère personnel, telles que celles utilisées pour l'identification biométrique à distance, est également considéré comme étant « à haut risque ».

▪ Le Contrôleur européen de la protection des données a qualifié les travailleurs de « groupe vulnérable » et suggéré un moratoire sur le traitement des données biométriques et comportementales (reconnaissance de caractéristiques humaines, pression des touches sur un clavier etc.) jusqu'à l'élaboration et la mise en place par les Etats d'un cadre juridique complet.

▪ En conférant le droit de ne pas être soumis à une décision fondée exclusivement sur un traitement automatisé (y compris le profilage), le règlement général sur la protection des données (RGPD) offre aux citoyens un important moyen de défense contre la mise en œuvre de l'IA dans le secteur des RH. Les autorités de protection des données se sont penchées sur le lien entre l'IA et prise de décision automatisée et ont publié des lignes directrices, soulignant l'importance des principes de transparence et d'explicabilité. En tout état de cause, les travailleurs doivent être sensibilisés à l'utilisation de ces technologies et correctement informés de l'existence d'une prise de décision automatisée, de la logique sous-jacente, ainsi que de l'importance et des conséquences prévues de ce traitement pour les travailleurs.

▪ Dans ce contexte, afin de les sauvegarder les droits, les libertés et les intérêts légitimes des travailleurs, le RGPD prévoit que les travailleurs ont, au minimum, le droit de demander une intervention humaine et le droit de contester cette décision.

▪ Les algorithmes d'IA ne sont pas parfaits, ils peuvent souvent être biaisés et, de ce fait, avoir des conséquences négatives sur la vie des personnes physiques, et notamment des travailleurs. Etant donné les risques juridiques que l'IA comporte, les employeurs mais, plus généralement, l'ensemble des organisations qui décident de recourir aux technologies d'IA, doivent traiter la question de la détection et l'atténuation des biais algorithmiques non seulement dès la conception de la solution d'IA choisie, au stade de son développement, mais également de manière permanente par la suite, tout au long du cycle de vie de cette solution.

GEORGE A.
BALLAS
&
THEODORE
KONSTANTAKOPOULOS

greece@
lexing.network

*Artificial Intelligence and Human Resources*

▪ *AI technologies have permeated important aspects of our lives and their use on commercial level has presented an opportunity for organisations for business development and productive restructuring. AI applications are increasingly being used in the Human Resources (HR) sector; however, this comes with certain legal risks, which management of organisations must be aware of and take into account when deciding to use AI tools and applications.*

▪ *The implementation of AI technologies in the HR sector can increase the efficiency (and arguably the fairness) of decision-making during the recruitment process, also can contribute to improvement of working conditions. The risks entailed are not negligible; algorithms can be opaque, when transparency and non-discrimination are statutory obligations and ethical priorities for organisations.*

▪ *AI in the HR sector can have a significant range of applications.*

- *It can, for instance, identify ideal candidates for certain roles, match job requirements with skills and experience, recommend jobs and roles to potential candidates, etc. Digital HR assistants are able to screen volumes of CVs and referrals, establishing patterns between candidates and persons who successfully undertook the same tasks before.*
- *Importantly, during interviews, AI tools can record reactions and posture of the interviewees and can assess and process factors that a human recruiter would not be able to (at least) easily identify and evaluate.*
- *AI tools can process market data and provide insights regarding the wages, the contract duration, etc., contributing this way to successful recruitment and management of valuable employees (e.g., translating personal data and behavioural signals into terms of productivity, efficiency and engagement with assigned duties).*

▪ *The implementation of AI technologies in HR is in the crossroads of data protection law, labour law and anti-discrimination regulations. The European Commission's "White Paper on Artificial Intelligence" delineates the European Union's approach to AI technologies and highlights the potential risks of AI in this sector. The use of AI for recruitment purposes is classified as "high risk" and regulatory guidance is offered with reference to specific safeguards (e.g. human oversight). In particular, processing of special (sensitive) categories of personal data, such as those used for remote biometric identification, is also considered as "high-risk" processing.*

▪ *Notably, the European Data Protection Supervisor (EDPS) has classified employees as "vulnerable group" and has suggested a moratorium on the processing of biometric and behavioural data (ranging from human features to keystrokes), until a comprehensive legal framework is developed and in place.*

- *The General Data Protection Regulation (GDPR) confers the right not to be subject to a decision solely based on automated processing (including profiling), establishing a significant regulatory defense in the implementation of AI in the HR sector. Data Protection Authorities have examined the connection between AI and automated decision-making and have published relevant guidelines, highlighting the importance of transparency and explainability. In all cases, employees need to be properly informed and aware of the use of such technologies, the existence of automated decision-making, its reasoning, the significance and the expected impact on the decision.*

- *In this context, the minimum suitable measures provided by GDPR to safeguard the employee's rights, freedoms and legitimate interests are the employee's right to request human intervention and the right to contest the decision.*

- *AI algorithms are not perfect, often can be biased and as such adversely impact the lives of individuals, including employees. Algorithmic bias detection and mitigation is not only an issue that needs to be addressed by design in the development stage, but, given the entailed legal risks, it should be, at all times, a priority and point of effort for employers and generally organisations using AI technologies.*

GEORGE A.
BALLAS
&
THEODORE
KONSTANTAKOPOULOS

greece@
lexing.network

## L'intelligence artificielle dans le domaine de la santé

▪ Alors que l'IA pourrait accroître de près de 957 milliards de dollars l'économie indienne d'ici 2035 **(1)**, l'Inde connait une forte augmentation des investissements, une hausse de création d'entreprises et une multiplication des applications dans le domaine de l'IA dans de nombreux secteurs. Cette croissance rapide est due à la fois aux fortes mesures d'incitations engagées par plusieurs états indiens en faveur des acteurs pour stimuler ce secteur et à l'infrastructure technologique déjà existante sur l'ensemble du territoire national. Grâce à un important soutien du gouvernement, l'un des principaux domaines d'activité de l'IA en Inde est le secteur de la santé (qui attire près de 8 % des investissements dans les start-up **(2)**), qui regroupe des opérateurs traditionnels du secteur des soins de santé, des jeunes poussés et de grandes multinationales.

▪ Actuellement dans le secteur de la santé, l'IA est principalement utilisée pour l'analyse prédictive, la détection précoce et le diagnostic personnalisé de diverses maladies, ainsi que pour l'amélioration du stockage et de l'analyse des données, de la chirurgie assistée et de la facilité d'accès aux soins médicaux. Dans ce contexte, le présent article présente une analyse synthétique du cadre juridique existant et se penche de manière prospective sur les changements législatifs qui pourraient avoir une incidence sur ce secteur.

### Cadre législatif existant

▪ D'une manière générale, le cadre législatif indien actuel dans le domaine de la santé concerne les domaines suivants :

- Protection des données : en Inde, les dossiers médicaux des personnes physiques sont qualifiés de « données ou informations personnelles sensibles » (« SPDI ») et leur collecte, stockage, sécurité, divulgation et transfert sont protégés par la loi. La violation de ces dispositions légales est sanctionnée par des dommages et intérêts ou des peines d'emprisonnement. Bien que les sous-traitants de données relèvent également de ces réglementations, leurs obligations se limitent au respect des normes de sécurité **(3)** prescrites par le cadre législatif, la responsabilité d'obtenir le consentement des personnes concernées incombant au responsable du traitement.
  Il est intéressant de noter que l'Inde ne dispose pas actuellement d'une législation spécifique concernant la protection des données de santé, et que les acteurs du secteur ont décidé d'adopter, par voie contractuelle, des normes mondiales, telles que celles prévues par la loi américaine en matière d'assurance maladie (« HIPAA »), pour les données de santé qu'ils collectent, y compris en ce qui concerne la pseudonymisation. Toutefois, si le traitement des données de santé peut conduire à l'identification d'un individu, ces informations peuvent être considérées comme des « données à caractère personnel » et bénéficier d'une protection législative, bien qu'à un degré moindre par rapport à une SPDI.

REFERENCES

(1) https://www.accenture.com/_acnmedia/PDF-68/Accenture-ReWire-For-Growth-POV-19-12-Final.pdf, consulté le 31-12-2020.

(2) FICCI-KPMG paper on "Indian Healthcare Start-ups-An inside look into funding", accessible à l'adresse http://ficci.in/study-page.asp?spid=20767&sectorid=18

(3) Par exemple, la norme IS/ISO/IEC 27001

- Propriété intellectuelle : Le régime de propriété intellectuelle en Inde n'admet pas la brevetabilité des algorithmes sur lesquels reposent le fonctionnement d'une solution d'IA. Toutefois, sous réserve de satisfaire au critère d'originalité, ces algorithmes peuvent bénéficier d'une protection en vertu de la loi sur le droit d'auteur.
- Interopérabilité : Le gouvernement indien a récemment institué l'autorité nationale de santé (NHA), un organisme chargé de la création, de la promotion et de la réglementation de l'écosystème de la santé numérique en Inde. Ses missions sont notamment de concevoir une stratégie, de construire une infrastructure technologique, de proposer des normes d'interopérabilité et de mettre œuvre une « mission nationale de santé numérique » en coordination avec les parties prenantes du gouvernement et de la société civile.

### Cadre législatif à venir

▪ Loi sur la sécurité des informations numériques dans la santé (« DISHA ») : Le projet de DISHA a été soumis à consultation publique afin de recueillir les commentaires des différentes parties prenantes. La DISHA vise à réglementer les établissements cliniques qui collectent, génèrent, transmettent ou stockent des données de santé numériques, et à établir une plateforme d'échange d'informations de santé pour encadrer davantage la collecte, le stockage et la transmission des données de santé numériques et des informations nominatives associées.

▪ Projet de politique de gestion des données de santé : Publié en août 2020, ce projet prévoit notamment la création d'un référentiel pour le traitement sécurisé des données personnelles et des données personnelles sensibles des personnes physiques dans le cadre de l' « écosystème national de santé numérique ». En outre, il prévoit la création d'un système de dossiers personnels et médicaux numériques facilement accessible aux individus et aux prestataires de services de santé, qui serait de nature purement volontaire et basé sur le consentement des personnes.

▪ Projet de loi sur la protection des données personnelles : A l'instar du RGPD de l'UE, ce texte en cours d'élaboration a pour ambition de changer le paradigme actuel et à fournir un cadre complet pour la collecte, le stockage et le traitement de toutes les données à caractère personnel. Le projet de loi introduit les principes de transparence et de responsabilité, tout en réitérant la nécessité d'appliquer des pratiques et de procédures de sécurité raisonnables. Il prévoit également des droits supplémentaires pour les personnes concernées, tels que le droit de confirmation et d'accès, de correction et d'effacement et le droit à la portabilité des données.

### Conclusion

▪ Bien que l'utilisation de l'IA dans le domaine de la santé ait connu une croissance phénoménale, force est de constater que l'arsenal législatif indien n'est pas encore suffisamment armé en termes de vie privée, de profilage et de protection des personnes. De nombreuses mesures législatives sont actuellement en cours pour encadrer la collecte et l'utilisation d'informations personnelles sensibles. Toutefois, les contours exacts de ces textes restent à confirmer.

SIDDHARTHA GEORGE
&
AMIT KIRAN
&
BILAL LATEEFI

india@
lexing.network



### *Artificial Intelligence in Health*

▪ *Proposed to add nearly USD 957 Billion to the Indian Economy by 2035* ***(1)****, India has seen a surge in investment, start-ups and implementation of artificial intelligence ("AI") across multiple sectors. This rapid growth has been a function of both strong Government incentives and the existing technology infrastructure of India, with several State governments providing attractive incentives and support infrastructure to players in this field. Prompted by strong Government support, one of the key areas of operations of AI remains the healthcare sector in India (attracting nearly eight percent (8%) of all monetary investment in startups* ***(2)****), with active participation from a mix of traditional healthcare operators, start-ups and large multinational players.*

▪ *As it presently stands, AI in this sector is primarily used for predictive analysis, early detection and personalised diagnosis of various diseases, in addition to ancillary improvements with respect to data storage and analysis, assistive surgery and easy access to medical care. In this context, we have briefly analysed the existing legal framework and anticipated legislative changes that would impact this sector.*

*(1) https://www.accenture.com/_acnmedia/PDF-68/Accenture-ReWire-For-Growth-POV-19-12-Final.pdf, last accessed on December 31, 2020.*

*(2) FICCI-KPMG paper on "Indian Healthcare Start-ups- An inside look into funding", available at http://ficci.in/study-page.asp?spid=20767&sectorid=18*

### *Existing Legislative Framework*

▪ *Broadly speaking, the present legislative framework provides for:*

- *Data Privacy: In India, the health records of any person are treated as sensitive personal data or information ("SPDI") and is afforded legislative protection vis-a-vis its collection, storage, security practices, disclosure and transfer. The consequences of failing to meet these standards range from penalties and compensatory damages to imprisonment. While data processors also fall within the ambit of these regulations, their obligations are limited to maintaining the security standards* ***(3)*** *prescribed under the legislative framework, with the responsibility of obtaining consent resting with the data collector.*

  *Interestingly, as India currently lacks specific legislation regarding the protection of healthcare information, industry players have contractually adopted global standards such as under the US Health Insurance Portability and Accountability Act ("HIPAA") for the healthcare information collected, including with respect to pseudo-anonymisation. However, it may be noted that if processing of healthcare information can lead to the identification of an individual, such information may be classified as 'personal data,' and is afforded legislative protection, albeit to a lesser degree compared to SPDI.*

*(3) IS/ISO/IEC 27001 is one such standard prescribed*

- *Intellectual Property: The intellectual property regime in India does not recognise patentability of algorithms, the basis on which an AI solution functions. However, subject to meeting the test of 'originality,' such algorithms may be entitled to protection under copyright law.*
- *Interoperability: Recently, the government of India created the National Health Authority (the "NHA"), an apex body responsible for creation, promotion and regulation of India's digital healthcare ecosystem. The NHA is responsible for designing strategy, building technological infrastructure, proposing standards of interoperability and implementation of a 'National Digital Health Mission' in coordination with stakeholders in the government and civil society.*

### *Upcoming Legislations*

▪ *Digital Information Security in Healthcare Act ("DISHA"): The draft of DISHA has been placed in public domain for comments from various stakeholders. DISHA aims to regulate clinical establishments who collect, generate, transmit or store digital health data, while also establishing a healthcare information exchange to further regulate the collection, storage and transmission of digital health data and associated personally identifiable information.*

▪ *Draft Health Data Management Policy. Released in August 2020, the draft policy inter alia provides for the creation of a framework for secure processing of personal and sensitive personal data of individuals as part of the proposed 'National Digital Health Ecosystem'. Additionally, it provides for the creation of a system of digital personal and medical health records which is easily accessible to individuals and health service providers which is purely voluntary in nature and based on the consent of individuals.*

▪ *Personal Data Protection Bill: Similar to the EU GDPR, this pending legislation looks to revamp the current paradigm and provides a comprehensive framework for collection, storage and processing of all personal data. The bill introduces the principles of transparency and accountability, while re-iterating the need for reasonable security practices and procedures. The bill also provides additional rights to data principals such as the right to confirmation and access, correction and erasure and data portability.*

### *Conclusion*

▪ *While there has been an astronomical growth in the use of AI in healthcare, it is clear that the legislative framework in India is yet to catch up with the potential issues around personal privacy, profiling and protection. However, multiple legislative measures have been proposed, which are likely to provide a framework for collection and usage of sensitive personal information, while maintaining appropriate safeguards. While drafts have been published, the exact contours of this framework remain to be seen.*

SIDDHARTHA GEORGE
&
AMIT KIRAN
&
BILAL LATEEFI

india@
lexing.network

## IA et voitures autonomes

### Introduction

▪ Il existe plusieurs définitions de l' « intelligence artificielle » :

- selon l'OCDE, l'intelligence artificielle est « un système automatisé qui, pour un ensemble donné d'objectifs définis par l'homme, est en mesure d'établir des prévisions, de formuler des recommandations, ou de prendre des décisions influant sur des environnements réels ou virtuels. Les systèmes d'IA sont conçus pour fonctionner à des degrés d'autonomie divers ».
- pour l'ICO, l'autorité britannique de protection des données, l'IA désigne, d'une part, dans la communauté des chercheurs en IA, « diverses méthodes d'utilisation d'un système non humain pour tirer des leçons de l'expérience acquise et imiter le comportement intelligent de l'homme », et, d'autre part, dans le contexte de la protection des données, « la théorie et le développement de systèmes informatiques capables d'exécuter des tâches nécessitant normalement une intelligence humaine ».

▪ Quelle que soit la définition retenue, elles font toutes deux ressortir une caractéristique très spécifique de l'IA : il s'agit d'une intelligence non humaine qui permet à un système ou à une machine d'imiter le comportement humain et de faire des prédictions ou de prendre des décisions qui auront une influence sur des vies humaines sur la base d'objectifs définis par les humains. Ces systèmes ou machines peuvent fonctionner avec un degré d'autonomie variable. Une machine utilisant l'IA est une machine qui a appris à fonctionner par elle-même et qui peut prendre des décisions sans intervention humaine, c'est pourquoi dans certains domaines, elle est considérée comme une entité supérieure, puisqu'il est peu probable qu'elle commette les erreurs que les humains vont, eux, inévitablement commettre.

### Voitures autonomes

▪ Les voitures sans conducteur sont désignées par le terme de « voitures autonomes ». La notion d'autonomie est, de fait, inhérente au concept d'IA. En effet, être autonome signifie « être indépendant et avoir le pouvoir de prendre ses propres décisions ». D'emblée, la similitude frappante avec le concept d'IA, à savoir le concept d'une machine qui peut décider seule, sans intervention humaine.

▪ Certes, dans les deux cas (c'est-à-dire dans le cas des voitures autonomes et de l'IA en général), ces systèmes sont développés et programmés par des humains et répondent à un ensemble très spécifique d'instructions définies par un programmeur. La capacité de ces machines à prendre leurs propres décisions ou à faire des prédictions est de fait basée sur des modèles mathématiques

développés par les humains. Cela dit, les systèmes d'IA, et notamment les voitures autonomes, prendront de toute évidence des décisions qui auront un impact significatif sur la vie des êtres humains. S'agissant des voitures autonomes, comme pour tout autre domaine, il est important de bien appréhender la nature et le type de ces décisions et leurs conséquences possibles, afin que leurs conséquences potentielles puissent être encadrées par la loi et dans l'intérêt des humains.

▪ Prenons quelques exemples :

- Supposons que je roule dans ma voiture autonome et qu'en cours de route, ma voiture s'approche d'une autre voiture qui a précédemment été impliquée dans plusieurs accidents et dont le conducteur est signalé dans la base de données des compagnies d'assurance comme un mauvais conducteur et comme un danger potentiel pour les autres véhicules : l'information concernant la proximité avec une voiture potentiellement dangereuse doit-elle être transmise au système de ma voiture ?
- Deuxième exemple : alors que je suis en route vers ma destination, les caméras vidéo de ma voiture autonome repèrent une autre voiture effectuant une manœuvre très dangereuse (un demi-tour sur une autoroute très fréquentée où les demi-tours sont interdits, ou bien le franchissement d'un feu tricolore, par exemple). Mes caméras vidéo ont enregistré la manœuvre et la plaque d'immatriculation du véhicule dangereux : cette information doit-elle être partagée ? avec qui ? En d'autres termes, toutes ces informations doivent-elles collectées et, si oui, seront-elles utilisées à des fins de profilage **(1)** ?

▪ Autrement dit, réglementer les situations décrites ci-dessus, et donc réglementer les voitures autonomes, revient à réglementer l'IA. La question suivante qui se pose est donc de savoir s'il possible, voire conseillé, de réglementer l'IA. Puisque les programmes d'IA ne sont rien d'autre qu'un ensemble d'algorithmes, comment le législateur peut-il réglementer un algorithme ? Comment un tribunal peut-il décider qu'un algorithme est contraire à la loi, et sur quelle base ?

### Voitures autonomes, données à caractère personnel et réglementation de l'IA

▪ Les voitures autonomes collectent une quantité énorme de données à caractère personnel. De nombreux modèles de voitures offrent des fonctions qui ont pour condition préalable l'accès aux informations personnelles de leurs propriétaires et l'enregistrement des données personnelles de leur environnement.

▪ Toutes les voitures autonomes sont équipées de caméras haute définition permettant d'avoir une vue complète (avant, arrière et latérale) du véhicule, capables d'enregistrer et d'envoyer des images de qualité parfaite. Dans certains cas, les caméras fonctionnent même lorsque la voiture n'est pas utilisée : un constructeur intègre par exemple un « mode sentinelle » qui active les caméras de la voiture lorsque celle-ci est garée, afin de prévenir les vols ou les dommages, et qui enregistre donc des images de passants totalement innocents. Un autre constructeur vante sur son site web les avantages du système d'assistance de son

(1) Le profilage, selon le RGPD, est « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».
Cette définition nous ramène à la définition de l'IA, qui est un système « en mesure d'établir des prévisions, de formuler des recommandations » sur la base d' « un ensemble donné d'objectifs définis par l'homme ».

véhicule qui, grâce à la réalité augmentée et sa navigation prédictive, « analyse vos habitudes et vous suggère les meilleurs hôtels et restaurants ».

▪ Lorsqu'elles sont utilisées, les voitures automatisées collectent une quantité importante de données sur des tiers (les autres véhicules et/ou les passants dont les images sont capturées par les caméras de la voiture). Ces personnes ne savent pas que leurs images et leurs données personnelles sont traitées. Dans le même temps, il est presque impossible de les en informer et de leur donner toutes les informations requises par la loi.

▪ Compte tenu de ces éléments, la question posée ci-dessus trouve une réponse positive : il est en effet nécessaire de réglementer les voitures autonomes, et donc de réglementer l'IA, puisque le traitement de données à caractère personnel est une caractéristique de base des systèmes de l'IA sur lesquels repose le fonctionnement des voitures autonomes.

▪ A cet égard, peu d'observateurs ont remarqué que le RGPD a discrètement introduit une réglementation de l'IA, qui s'applique aussi aux voitures autonomes :

- Tout d'abord, le RGPD impose de traiter le moins de données personnelles possible en vertu du principe de minimisation des données, un principe qui semble difficilement compatible avec les programmes d'AI qui ont au contraire généralement besoin d'une grande quantité de données pour accomplir leurs tâches (2).
- Ensuite, le RGPD exige que la personne concernée soit informée du traitement, en recevant des « informations utiles » sur le traitement et « la logique sous-jacente ». Dans le cas d'une voiture autonome, comment sera-t-il possible d'informer tous les passants et les conducteurs des autres véhicules qui, comme expliqué ci-dessus, ne savent pas que leurs images et leurs données à caractère personnel sont traitées par le véhicule autonome ?
- Enfin, le responsable du traitement doit obligatoirement effectuer une analyse d'impact relative à la protection des données (AIPD) lorsque le traitement utilise de grands volumes de données à caractère personnel pour établir un profilage des utilisateurs. Si l'AIPD indique que le traitement présente un risque élevé, une consultation préalable de l'autorité locale de protection des données est nécessaire.

▪ Ainsi, la question du traitement des données à caractère personnel par l'AI est assez épineuse. Comme nous l'avons vu, il existe plusieurs obstacles à surmonter et le RGPD contient des règles assez strictes (sans parler des fortes amendes encourues). Il faut dire que la question de la gouvernance et de la réglementation de l'IA est elle-même très complexe. L'OCDE a publié des lignes directrices sur le développement de l'IA, mais il ne s'agit que d'orientations. À ce stade, le RGPD a un impact beaucoup plus important, puisque sa nature législative dans les pays de l'UE impose son respect.

▪ Le RGPD prépare également le terrain pour les outils d'autorégulation. Outre une AIPD, le RGPD prévoit la mise en œuvre de codes de conduite, c'est-à-dire un ensemble de règles standard « destiné[e]s à contribuer à la bonne application du

(2) Le considérant 71 du RGPD indique que « le responsable du traitement devrait utiliser des procédures mathématiques ou statistiques adéquates aux fins du profilage, appliquer les mesures techniques et organisationnelles appropriées pour faire en sorte, en particulier, que les facteurs qui entraînent des erreurs dans les données à caractère personnel soient corrigés et que le risques d'erreur soit réduit au minimum ».
Mais, pour éviter toute confusion ou malentendu, ce considérant poursuit en précisant que ce programme doit être élaboré « d'une manière qui tienne compte des risques susceptibles de peser sur les intérêts et les droits de la personne concernée et qui prévienne, entre autres, les effets discriminatoires à l'égard des personnes physiques fondées sur la l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions, l'appartenance syndicale, le statut génétique ou l'état de santé, ou l'orientation sexuelle, ou qui se traduisent par des mesures produisant un tel effet. La prise de décision et le profilage automatisés fondés sur des catégories particulières de données à caractère personnel ne devraient être autorisés que dans des conditions spécifiques »

[RGPD], compte tenu de la spécificité des différents secteurs de traitement ». Le code de conduite présente des avantages importants, car son contenu n'est pas défini par un tiers non spécialisé, même s'il doit tout de même être approuvé par l'autorité nationale, voire par le CEPD lorsqu'il concerne un traitement de données à caractère personnel qui a lieu dans plusieurs États. En pratique, avec ce système, les acteurs du secteur ont ainsi la possibilité de débattre des meilleures pratiques à adopter, de les négocier et d'en esquisser les contours de manière à limiter l'impact potentiel qu'une interprétation stricte des règles pourrait avoir sur le développement du secteur.

## Conclusion

▪ En résumé, le RGPD a établi des normes raisonnables pour réglementer l'IA, combinant des prescriptions obligatoires et un système d'autorégulation et de coopération avec les autorités. Il faut espérer que ces normes permettront le développement d'un ensemble commun de règles pour encadrer l'IA, et plus particulièrement les traitements de données à caractère personnel mis en oeuvre par l'IA dans le secteur automobile.

RAFFAELE ZALLONE

italy@
lexing.network

*AI & Autonomous Cars*

*Introduction*

- *There are several definitions of "artificial intelligence":*

  - *according to the OECD artificial intelligence is: "a machine-based system that can, for a human defined set of objectives, make predictions, recommendations or decisions influencing real or virtual environments. AI systems are designed to operate with different levels of autonomy".*

  - *the ICO (the UK Data Protection Authority) defines AI as follows: "In the AI research community, it refers to various methods for using a non-human system to learn from experience and imitate human intelligent behavior; or in the data protection context, 'the theory and development of computer systems able to perform tasks normally requiring human intelligence".*

- *Whatever the definition one may prefer, they both point to one very specific characteristic: it's a non-human intelligence that allows a system or a machine to imitate human behavior and make predictions or decisions that will have an influence on human lives on the basis of objectives defined by humans; in addition such systems or machines can operate with some variable degree of autonomy. Any machine using AI is a machine that has learned to operate on its own and can make decisions without human intervention, hence in certain domains it is considered as a superior entity, since it is unlikely to make the same mistakes humans can inevitably make.*

*Autonomous cars*

- *Now I would like to bring your attention to the name given to cars that do not need a driver: autonomous cars. The concept of autonomy is somehow included in the concept of AI: in fact autonomous means "independent and having the power of making your own decisions". This definition shows a striking similarity with the concept of AI, that is to the concept of a machine that can decide on its own, without the need for human intervention.*

- *The truth of the matter is that in both cases (i.e. in the case of autonomous cars and of AI in general) we have systems that have been developed and programmed by humans and that respond to a very specific set of instructions defined by a programmer. The capacity of these machines to make their own decisions or predictions is based on mathematical models developed by humans. Having said this, it is clear that AI systems, including autonomous cars, will be making decisions that shall have significant impact on the lives of human beings; as in any other field, in the case of autonomous cars it is important to understand what these decisions*

*may be and their possible consequences, so that their potential impact may be addressed and disciplined according to the law and to the advantage of us humans.*

▪ *Let's make a few examples:*

- *Assume that on my way to destination I am riding in my autonomous car. Along the route my car gets on the same path and/or follows or otherwise gets close to a car which has been involved in several accidents and whose driver is marked in the insurance companies system as a poor driver and a potential danger for other cars: shall the information about being close to a potentially dangerous car be shared with the system of my car?*

- *Second example: while cruising to destination the video cameras of my car spot another car performing a highly dangerous maneuver (e.g.: a U-turn on a highly trafficked freeway, where U-turns are forbidden, or running a red light). The video camera has recorded the maneuver and the license plate: shall this information be shared and with whom? In other words, will all such information be collected, and if so, will they be used to create a profile? **(1)***

▪ *This means that regulating such situations and regulating autonomous cars means regulating AI The next question then is: is it possible, and indeed advisable to regulate AI? And since AI programs are nothing but a set of algorithms, how can a legislator regulate an algorithm? And how can a Court decide that an algorithm is against the law, and on what basis?*

*Autonomous cars, personal data and AI regulation*

▪ *Autonomous cars collect an enormous amount of personal data; many car models offer functions that have as a prerequisite the access to personal information about their owners and which are capable to record personal data available in the surroundings.*

▪ *All such cars have installed high-definition tele-cameras, covering front, side and back of the car which can record and sent perfect images. In some cases, the cameras work also when the car is not being used: one manufacturer has a "sentry mode" that activates the cameras when the car is parked, to prevent theft or damages, hence recording images of totally innocent by-standers. Another manufacturer when in its website describes its assistance system, taunts its augmented reality and predictive navigation, "that analyze your habits and suggest the best hotels and restaurants".*

▪ *When in use, automated cars collect a significant amount of information of unrelated third parties (other vehicles and/or the by-standers whose images are captured by the cameras of the car). These persons are not in a condition to know that their images and personal data are being processed; at the same time it is almost impossible to give them all the information required by the law.*

*(1) Profiling, according to the GDPR, is "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements".*
*This definition brings us back to the definition of A.I, which is a system that "can make predictions, recommendations or decisions" on the basis of "a human defined set of objectives".*

▪ *All these facts and circumstances answer the question asked above: is it necessary to regulate autonomous cars: it is indeed necessary to regulate AI, since the processing of personal information is a basic feature of the AI systems on whose basis autonomous cars operate.*

▪ *Not too many observers have noticed that the GDPR has quietly introduced a regulation of AI, which obviously applies to autonomous cars as well:*

- *First, GDPR requires to process as little personal data as possible (the so-called data minimization principle) a principle that seems at odds with the programs that will control the operations of AI, which usually require large amount of data to perform their tasks* ***(2)****.*

- *Second: it is well known that the GDPR requires the data subject be informed of the processing, in fact must receive "meaningful information" about the processing and "the logic involved". How will be possible to inform all the bystanders and the drivers of the other vehicles that, as mentioned above, do not know that their images and personal data are being processed?*

- *Finally, the controller must also perform a data protection impact assessment (DPIA), which is mandatory if the processing uses high volumes of personal data to profile users; should the DPIA result in the evaluation of a high-risk processing, prior consultation with the local Data Protection Authority (DPA) is needed.*

▪ *It is clear that the problem of processing personal data in the context of AI is quite complex. As we have seen, there are several obstacles to tackle and the GDPR has quite strict rules (not to mention the fines). At the same time, the question of governing and regulating AI is as well quite complex. The OECD has published its guidelines on the development of AI, but they are only guidelines. At this point, the GDPR has a much stronger impact, since it is a law of the land to be complied with.*

▪ *Let's not forget that the GDPR also sets the stage for self-regulation tools. In addition to the DPIA, the GDPR calls for the implementation of codes of conduct, a set of standard rules to be used "intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors". Codes of conduct have significant advantages: the rules are not defined by an unrelated third party, but have to be approved by the authority and in case a code of conduct relates to processing of personal data that takes place in several states, it must be approved by the EDPB. This means, in practice, a negotiation where the industry can explain the best practices to be adopted, trying to sketch them in such a way as to limit the potential impact that strict interpretation of the rules may have on the development of the industry.*

(2) *Recital 71 states that "the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organizational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimized". But just to avoid any confusion or misunderstanding, the wording continues stating that the program must be developed in a way "that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions."*

*Conclusion*

▪ *The sum of all this is that we must be aware that the GDPR has set very reasonable standards to regulate AI, with a mix of clear prescriptions, self-regulations and cooperation with the Authorities which, hopefully, will allow the development of a common set of rules to be used for the regulation of AI and for the governing of the processing of personal data in this new area of business.*

RAFFAELE ZALLONE

italy@
lexing.network

| PAYS / COUNTRY | CABINET / FIRM | CONTACT | TELEPHONE | EMAIL |
|---|---|---|---|---|
| Afrique du Sud *South Africa* | Michalsons | John Giles | +27 (0) 21 300 1070 | south-africa@lexing.network |
| Allemagne *Germany* | Beiten Burkhardt | Andreas Lober | +49 69 756095-0 | germany@lexing.network |
| Australie *Australia* | Gadens | Dudley Kneller | +61 438 363 443 | australia@lexing.network |
| Belgique *Belgium* | Lexing Belgium | Jean-François Henrotte | +32 4 229 20 10 | belgium@lexing.network |
| Canada *Canada* | Langlois avocats, S.E.N.C.R.L. | +1 514 282 7817 | +1 (418) 650 7000 | canada@lexing.network |
| Chine *China* | Jade & Fountain PRC Lawyers | Jun Yang | +86 21 6235 1488 | china@lexing.network |
| Côte d'Ivoire *Ivory Coast* | Imboua Kouao Tella & Associés | Annick Imboua-Niava | + 225 22 44 74 00 | ic@lexing.network |
| Espagne *Spain* | Lexing Spain | Marc Gallardo | + 34 93 476 40 48 | spain@lexing.network |
| États-Unis *USA* | DataMinding Legal Services | Françoise Gilbert | +1 650-804-1235 | usa@lexing.network |
| France *France* | Alain Bensoussan-Avocats Lexing | Alain Bensoussan | +33 1 82 73 05 05 | france@lexing.network |
| Grèce *Greece* | Ballas, Pelecanos & Associates L.P.C. | George A. Ballas | + 30 210 36 25 943 | greece@lexing.network |
| Guinée *Guinea* | BAO & Fils | Mody Oumar Barry | + 224 623 68 78 79 | guinea@lexing.network |
| Hongrie *Hungary* | OPL - Orbán & Perlaki | Miklos Orban | +36 1 244 8377 | hungary@lexing.network |
| Inde *India* | Poovayya and Co | Siddhartha George | +91 80 4115 6777 | india@lexing.network |
| Italie *Italy* | Studio Legale Zallone | Raffaele Zallone | + 39 (0) 229 01 35 83 | italy@lexing.network |
| Japon *Japan* | Hayabusa Asuka Law Office | Koki Tada | +81 3 3595 7070 | japan@lexing.network |
| Liban *Lebanon* | Kouatly & Associates | Rayan Kouatly | + 961 175 17 77 | lebanon@lexing.network |
| Maroc *Morocco* | Elkhatib Lawfirm | Hatim Elkhatib | +212 5 39 94 05 25 | morocco@lexing.network |
| Mexique *Mexico* | Carpio, Ochoa & Martínez Abogados | Enrique Ochoa De Gonzälez Argüelles | + 52 55 25 91 1070 | mexico@lexing.network |
| Norvège *Norway* | Advokatfirmaet Føyen Torkildsen AS | Arve Føyen | +47 21 93 10 00 | norway@lexing.network |
| Nouvelle-Calédonie *New Caledonia* | Cabinet Franck Royanez | Franck Royanez | + 687 24 24 48 | nc@lexing.network |
| République tchèque *Czech Republic* | Rowan Legal | Josef Donát Michal Nulíček | +420 224 216 212 | czechrepublic@lexing.network |
| Royaume-Uni *United Kingdom* | Preiskel & Co LLP | Danny Preiskel | + 44 (0) 20 7332 5640 | uk@lexing.network |
| Sénégal *Senegal* | SCP Faye & Diallo | Mamadou Seye | :(+221) 33 823 60 60 | senegal@lexing.network |
| Slovaquie *Slovakia* | Rowan Legal | Josef Donát Michal Nulíček | +420 224 216 212 | slovakia@lexing.network |
| Suisse *Switzerland* | Sébastien Fanti | Sébastien Fanti | + 41 (0) 27 322 15 15 | switzerland@lexing.network |

La JTIT est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris, président : Alain Bensoussan. Directeur de la publication : Alain Bensoussan – Responsable de la rédaction : Isabelle Pottier Diffusée uniquement par voie électronique – gratuit– ISSN 1634-0701
Abonnement à partir du site : https://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-debat/