PREISKEL & CO

BIOMETRIE ET RECONNAISSANCE FACIALE
BIOMETRICS AND FACIAL RECOGNITION

PROTECTION DES DONNEES ET PRATIQUE DES AUTORITES DE CONTROLE

- La biométrie regroupe, selon la définition donnée par la Cnil, l'ensemble des procédés automatisés permettant de reconnaître un individu à partir de la quantification de ses caractéristiques physiques, physiologiques ou comportementales (empreintes digitales, réseau veineux, iris, etc.). Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne.
- La reconnaissance faciale, notamment, présente beaucoup d'intérêt en matière de sûreté et de sécurité, mais elle est aussi porteuse d'un risque important d'atteinte aux libertés individuelles. C'est pourquoi, en France, la Cnil a appelé à un débat démocratique sur ces technologies. Au sein de l'Union européenne, l'utilisation de tels dispositifs est encadrée par le règlement général sur la protection des données (RGPD). En outre, la Commission européenne prépare un règlement qui autorisera les citoyens de l'Union européenne à contrôler l'utilisation de leurs données de reconnaissance faciale.
- Quels sont les risques technologiques, éthiques, sociétaux, liés à ces technologies ? Quel cadre juridique s'applique aux dispositifs de reconnaissance faciale ? Quelles mesures sont prises par les autorités de régulation dans le monde pour les sécuriser, établir un cadre de confiance et développer des bonnes pratiques ?

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, Allemagne, Belgique, France, Grèce, Italie.

DATA PROTECTION ISSUES AND PRACTICE OF LOCAL DPAS

- *Biometrics, according to the CNIL, includes all automated processes used to recognise an individual by quantifying their physical, physiological or behavioural characteristics (fingerprints, blood vessel patterns, iris structure, etc.). Biometric data are personal data because they make it possible to identify that individual.*
- *Facial recognition, in particular, is of great interest in terms of safety and security, but it also poses significant risks for individual freedoms. In France, the CNIL called for a democratic debate to be held on these technologies. In the European Union, the use of such devices is governed by the General Data Protection Regulation (GDPR). In addition, the European Commission is preparing a regulation that will give EU citizens control over the use of their facial recognition data.*
- *What are the technological, ethical and societal risks associated with these technologies? What is the legal framework governing facial recognition devices? What measures are being taken in various countries around the world to secure them, build consumer trust and develop good practices?*

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

ALAIN BENSOUSSAN
Fondateur et président
Lexing Alain Bensoussan-Avocats
Fondateur et président du réseau Lexing®

Founder and Managing Partner
Lexing Alain Bensoussan-Avocats
Founder and President of the Lexing® network

LEXING
ALAIN BENSOUSSAN AVOCATS

AFRIQUE DU SUD

MICHALSONS

▪ En Afrique du Sud, les empreintes digitales et le groupe sanguin d'une personne étaient auparavant protégés en tant que « données à caractère personnel » sous l'empire de la loi sur les communications et les transactions électroniques (1). Elles le seront bientôt en tant que « données biométriques ». En effet, la future loi sur la protection des données à caractère personnel (POPIA), qui n'est pas encore complètement entrée en vigueur, intègre désormais le terme « biométrie », qu'elle définit comme une « technique d'identification d'une personne à partir de ses caractéristiques physiques, physiologiques ou comportementales, notamment le groupe sanguin, les empreintes digitales, l'analyse d'ADN, l'empreinte rétinienne et la reconnaissance vocale » (2).

▪ La POPIA va donc plus loin, en ce qu'elle protège les données biométriques en tant que catégorie particulière de données à caractère personnel. Si la POPIA édicte une interdiction générale de traiter des données biométriques (3), elle aménage cependant, dans le même temps, plusieurs exceptions à cette interdiction en accordant, par exemple, une autorisation générale de traitement de catégories particulières de données à caractère personnel dans la mesure où certaines conditions sont remplies (4), ainsi qu'une autorisation spécifique de traitement concernant les données biométriques et les comportements criminels (5). Cette autorisation spécifique, strictement encadrée, permet aux forces de l'ordre et aux responsables du traitement de mettre en œuvre le traitement de données biométriques sous réserve du respect des dispositions légales et particulièrement de la réglementation en matière de droit du travail.

▪ Il en ressort que, hormis dans le domaine de la police et du droit du travail, l'utilisation des données biométriques requiert obligatoirement le recueil du consentement. En effet, le consentement constitue le seul cas prévu par l'autorisation générale sur laquelle on puisse se fonder dans la pratique.

Exemples d'usages de la biométrie en Afrique du Sud

▪ Actuellement, la biométrie est utilisée aussi bien par des personnes publiques (l'Etat) que privées (banques) pour des applications mobiles, des dispositifs de contrôle d'accès… L'une des techniques biométriques les plus utilisées est l'empreinte digitale, mais l'usage de la reconnaissance vocale et de la reconnaissance faciale est en constante augmentation.

Opinion publique

▪ La population sud-africaine semble favorable à l'utilisation de la biométrie, et davantage sensible aux bénéfices apportés par celle-ci en termes de sécurité qu'aux inquiétudes qu'elle peut soulever concernant à protection de la vie privée (6).

Protection des données

▪ Instaurée par la POPIA, l'autorité de protection des données sud-africaine n'en est qu'à un stade embryonnaire et n'a pas encore formulé de recommandations ou de décisions spécifiques relatives la biométrie. C'est donc vers l'Union européenne que les Sud-Africains se tournent pour l'instant pour obtenir des orientations en la matière.

REFERENCES

(1) Loi 25 de 2002 accessible à l'adresse : https://www.gov.za/sites/default/files/gcis_document/20140 9/a25-02.pdf

(2) Loi 4 de 2013 accessible à l'adresse : https://popia.co.za/section-1-definitions/

(3) Section 26 https://popia.co.za/section-26-prohibition-on-processing- of-special-personal- information/

(4) Section 27 https://popia.co.za/section-27-general-authorisation-concerning-special-personal- information/

(5) Section 33 https://popia.co.za/section-33-authorisation-concerning- data-subjects-criminal- behaviour-or-biometric- information/

(6) Comme le montre une étude sur l'utilisation de l'IA et des caméras : https://www.businesslive.co.za/fm/features/2019-06-13-surveillance-state-big-brother- lands-in-joburg/

SARAH BUERGER
&
JOHN GILES

south-africa@lexing.network

SOUTH AFRICA

MICHALSONS

▪ *South Africa previously protected fingerprints and a person's blood type as personal information under the Electronic Communications and Transactions Act (1). The term 'biometrics' was introduced in the Protection of Personal Information Act (POPIA) (which still has not fully commenced as yet). POPIA defines biometrics as a 'technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition' (2).*

▪ *The Act goes further and protects biometric information as special personal information. This means that there is a general prohibition on processing biometric information in South Africa (3). POPIA then gives a general authorisation for the processing of special personal information (4), and a specific authorisation of processing criminal behaviour or biometric information (5). The specific authorisation is very limited, and allows for law enforcement and responsible parties (controllers) to process biometrics if they are doing so in accordance with the law and with labour legislation.*

▪ *These authorisations indicate that the potential use of biometrics beyond law enforcement and the employment realm will always require consent (as this is the only general authorisation that can practically be relied upon).*

Examples of biometrics in South Africa

▪ *Currently biometrics are used by Government, banks, Apps and access control in various organisations. Generally fingerprints are the most commonly used type, but we have seen voice recognition and facial recognition being used more.*

Public perception

▪ *The South African public seems to favour safety over privacy concerns (6).*

Data Protection

▪ *The Data Protection Authority in South Africa is still in its infancy, and has not made any recommendations or rulings based on biometrics. South Africans therefore look to the European Union for guidance in this matter.*

REFERENCES

(1) Act 25 of 2002 available at https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf

(2) Act 4 of 2013 available at https://popia.co.za/section-1-definitions/

(3) Section 26 https://popia.co.za/section-26-prohibition-on-processing-of-special-personal-information/

(4) Section 27 https://popia.co.za/section-27-general-authorisation-concerning-special-personal-information/

(5) Section 33 https://popia.co.za/section-33-authorisation-concerning-data-subjects-criminal-behaviour-or-biometric-information/

(6) As shown by a study into the use of AI and cameras. https://www.businesslive.co.za/fm/features/2019-06-13-surveillance-state-big-brother-lands-in-joburg/

SARAH BUERGER
&
JOHN GILES

south-africa@lexing.network

▪ A mesure que les systèmes de traitement des données biométriques se développent, ils attisent la curiosité du grand public et attire la vigilance des autorités de protection des données. Si les entreprises s'enthousiasment des avantages offerts par cette nouvelle technologie, les autorités de contrôle sont plus réservées. En effet, les données biométriques sont des catégories particulières de données à caractère personnel au sens de l'article 9, paragraphe 1, du RGPD et, à ce titre, leur traitement à des fins d'identification est soumis au respect d'exigences particulièrement strictes.

▪ Plusieurs autorités allemandes de protection des données ont d'ailleurs d'ores et déjà inscrit, conformément à l'article 35, paragraphe 4, du RGPD, les traitements des données biométriques à leur « liste noire » regroupant les opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.

▪ Ainsi, l'autorité bavaroise de protection des données requiert la réalisation d'une analyse d'impact même lorsque le traitement des données biométriques ne satisfait qu'un seul des critères posés par le groupe de travail « Article 29 » dans ses lignes directrices concernant la manière de déterminer si un traitement nécessite une AIPD. (1)

▪ L'autorité de protection des données de Berlin semble suivre une approche similaire. (2) De fait, l'autorité berlinoise a explicitement inclus dans sa liste noire les systèmes de contrôle d'accès ou de paiement par empreintes digitales, domaines d'application de prédilection des données biométriques.

▪ Par conséquent, le traitement de données biométriques en Allemagne nécessitera généralement la réalisation d'une analyse d'impact sur la protection des données, quand bien même une telle analyse n'est pas explicitement requise par le RGPD.

▪ Dans son rapport d'activité de 2019, le commissaire à la protection des données et à la liberté d'information de Hambourg constate l'utilisation croissante des données biométriques pour l'authentification en ligne et l'authentification des paiements. (3) Il relève que cette utilisation enfreint souvent le principe de minimisation des données et s'interroge sur la fiabilité des systèmes d'authentification basés sur des données biométriques. Compte tenu de l'impossibilité d'obtenir une correspondance exacte du gabarit stocké avec les caractéristiques biométriques scannées de la personne concernée, il souligne que la correspondance obtenue repose alors exclusivement sur des paramétrages prédéfinis. La personne concernée n'est donc identifiée qu'avec un certain degré de probabilité. En revanche, le risque d'abus, au détriment de la personne concernée, est lui très élevé. Avec seulement quelques photos, il est en principe possible de reconstituer les caractéristiques biométriques du visage d'un individu. En outre, si ces données biométriques sont perdues, elles ne pourront plus jamais être utilisées (en toute sécurité) par cette personne à des fins d'identification.

▪ Déterminées à encadrer les traitements des données biométriques, les autorités allemandes de protection des données ont pris le problème à bras le corps : la police de Hambourg utilisait un logiciel de reconnaissance faciale automatisé qui analysait des données vidéo et images (stockées dans une base de données de plus de 32.000

(1) https://www.datenschutz-bayern.de/datenschutzreform2018/DSFA_Blacklist.pdf

(2) https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/datenschutzfolgeabschaetzung/BlnBDI-2018-DSFA-nicht-oeffentlich.pdf

(3) https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf (page 142)

fichiers) afin d'aider l'enquête sur les infractions commises lors du sommet du G20 en juillet 2017. A l'issue d'un examen des traitements opérés à l'aide de ce logiciel, le commissaire à la protection des données de Hambourg a estimé qu'ils ne reposaient sur aucune base juridique et ordonné la suppression de la base de données. (4) Le tribunal administratif a, toutefois, déclaré illégale la décision prononcée par le commissaire à la protection des données en raison d'erreurs commises commise dans la procédure administrative. (5) Pour autant, le tribunal n'a pas déclaré le traitement des données biométriques recevable. Ce jugement n'est pas encore définitif.

▪ Il existe néanmoins déjà une décision de justice exécutoire en matière d''utilisation d'outils biométriques. Le tribunal du travail de Berlin a statué que l'utilisation d'un système d'empreintes digitales pour enregistrer les heures de travail des employés nécessitait le consentement des employés, aux motifs que ce système n'était pas nécessaire aux fins de la relation de travail (6). Dans le même temps, le tribunal a précisé que l'utilisation des données biométriques des employés pour le contrôle d'accès à des zones de travail spécifiques (par exemple, les pièces où sont stockées des secrets d'affaires) pouvait être légitime.

▪ Au vu des premières décisions rendues par les tribunaux et des actions engagées par les autorités chargées de la protection des données, il convient de procéder au cas par cas afin de décider si l'utilisation de systèmes de traitement des données biométriques est possible d'une manière respectueuse de la vie privée et des données, et d'identifier les exigences à satisfaire en matière de protection des données.

(4) https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf (page 98f)

(5) https://justiz.hamburg.de/aktuellepresseerklaerungen/13105802/pressemitteilung/

(6) http://www.gerichtsentscheidungen.berlin-brandenburg.de/jportal/portal/t/hnm/bs/10/page/sammlung.psml;jsessionid=9D87BBC2862239923F57C1651466402A.jp21?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=1&numberofresults=1&fromdoctodoc=yes&doc.id=JURE190016085&doc.part=L&doc.price=0.0#focuspoint

SUSANNE KLEIN
&
LENNART KRIEBEL

germany@lexing.network

▪ *With the spread of biometric data processing tools, not only the public's awareness of them is increasing, but also that of the German data protection authorities. While companies are often enthusiastic and would like to use the new technology, data protection authorities are rather skeptical about it. The reason for this is that biometric data are special categories of personal data within the meaning of Article 9 (1) GDPR and their processing for identification purposes is therefore subject to particularly strict requirements.*

▪ *Several German data protection authorities have already added the processing of biometric data to their blacklist under Article 35 (4) GDPR.*

▪ *The data protection authority of Bavaria stipulates the conduction of a data protection impact assessment even when the processing of biometric data is subject to a single additional criterion under the guidelines of the Article 29 Working Party. (1)*

▪ *The Berlin data protection authority seems to pursue a similar approach. (2) Typical fields of implementation of biometric data, such as access control systems or payments by fingerprint, are explicitly covered by the Berlin blacklist.*

▪ *Therefore, if biometric data is processed in Germany, a data protection impact assessment must usually be conducted, even when it is not explicitly required by GDPR.*

▪ *The Hamburg Commissioner for Data Protection and Freedom of Information states in its 2019 activity report that biometric data is increasingly used for online and payment authentication. (3) He indicates that such use often infringes the principle of data minimization, and questions the reliability of authentication systems based on biometrical data. Since an exact match of the stored template with the (respective) scanned biometric characteristics of the data subject is not possible, the match depends exclusively on predefined tolerances. Identification of the data subject is therefore only possible with a certain degree of probability. In contrast, the risk of abuse is very high for the data subject. With only a few photos it is basically possible to reconstruct biometric characteristics of a data subject's face. Additionally, if the biometric data are lost, these data can never again be (safely) used by the data subject for identification purposes.*

▪ *The German data protection authorities have already begun to take action against the processing of biometric data: The Hamburg police authority used to run an automatic facial recognition software which evaluates video and image data (stored on a database of over 32,000 files) to investigate crimes committed during the G20 summit in July 2017. The Hamburg Data Protection Commissioner reviewed the procedure, concluded there was no legal basis for the processing*

(1) *https://www.datenschutz-bayern.de/datenschutzreform2018/DSFA_Blacklist.pdf*

(2) *https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/datenschutzfolgeabschaetzung/BlnBDI-2018-DSFA-nicht-oeffentlich.pdf*

(3) *https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf (page 142)*

activities and ordered the deletion of the database. (4) The Administrative Court, however, declared this order unlawful due to errors made by the data protection authority in the administrative procedure. (5) The court did not declare the processing of biometric data to be admissible, though. The ruling is not yet final.

▪ *Nonetheless, there is already a legally binding court decision on the use of biometric tools. The Berlin Labor Court has ruled that the use of a fingerprint system to record the working hours of employees requires the employees' consent as it is not necessary for the purposes of the employment relationship.(6) However, the court also indicated that the use of biometric data of employees for access control to specific office areas (e.g. where business secrets are stored) may be legitimate.*

▪ *In view of these first decisions and actions of the DPAs, it will always depend on the specific individual case in order to decide whether the use of biometric data processing systems is possible in a data protection-compliant manner and which data protection requirements have to be met.*

(4) https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf (page 98f)
(5) https://justiz.hamburg.de/aktuellepresseerklaerungen/13105802/pressemitteilung/
(6) http://www.gerichtsentscheidungen.berlin-brandenburg.de/jportal/portal/t/hnm/bs/10/page/sammlung.psml;jsessionid=9D87BBC2862239923F57C1651466402A.jp21?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=1&numberofresults=1&fromdoctodoc=yes&doc.id=JURE190016085&doc.part=L&doc.price=0.0#focuspoint

SUSANNE KLEIN
&
LENNART KRIEBEL

germany@lexing.network

BELGIQUE

LEXING BELGIUM

Reconnaissance faciale : traitement de données biométriques

▪ Bien qu'elle ne se soit pas (encore) précisément prononcée sur la question de la reconnaissance faciale, l'Autorité de protection des données belge (« APD ») apporte des éclairages sur le traitement des données biométriques. Le processus de reconnaissance faciale implique, en effet, des données qui sont liées au propre corps de l'individu / personne concernée (voir l'article 4, 14° du RGPD).

Avis n°17/2008 de l'APD : authentification de personnes

▪ L'Autorité (« Commission pour la Vie Privée », avant décembre 2017) a rendu un avis (1) concernant le traitement des données biométriques, uniquement dans le cadre de l'authentification des personnes. Ce procédé permet ainsi au responsable du traitement de vérifier qu'une personne est bien celle qu'elle prétend être (dans le cadre d'un contrôle d'accès). Outre cette fonction d'authentification, la reconnaissance faciale permet également d'identifier les individus (retrouver une personne dans une foule par exemple).

Règlement général sur la protection des données et la loi du 30 juillet 2018

▪ Même si cet avis de l'APD reste utile, il ne reflète plus la situation actuelle en la matière. En effet, depuis l'entrée en application du RGPD, le traitement de données biométriques connaît un cadre légal plus strict :

- Article 9 du RGPD (2) : Sur base de cette disposition, les données biométriques sont des données sensibles. Dès lors, le principe veut que le traitement de telles données soit interdit. Néanmoins, le paragraphe 2 de ladite disposition prévoit que le responsable du traitement peut traiter ces données dans plusieurs hypothèses. Il est intéressant de noter que le fondement tenant à l'intérêt légitime du responsable du traitement ne figure pas parmi les exceptions du § 2.
- Article 9 de la loi du 30 juillet 2018 (3) : Se fondant sur l'article 9, § 4 du RGPD, le législateur belge a ajouté une condition au traitement de données biométriques. Il est ainsi prévu, à l'article 9 de la loi du 30 juillet 2018, que le responsable du traitement doit prendre des mesures supplémentaires lorsque des données, notamment, biométriques sont traitées. Ces mesures, qui sont au nombre de trois, consistent à désigner précisément les personnes qui ont accès aux données biométriques, à communiquer la liste de leur identité à l'APD et veiller à ce que ces personnes soient tenues au respect du caractère confidentiel de ces données, par une obligation légale ou par une disposition contractuelle équivalente.

▪ Analyse d'impact relative à la protection des données obligatoire

Enfin, l'APD a communiqué un Avis (4) dans lequel elle liste les traitements de données pour lesquels une analyse d'impact est obligatoire. Ainsi, telle analyse doit être menée lorsque le traitement utilise des données biométriques en vue de l'identification unique des personnes concernées se trouvant dans un lieu public ou dans un lieu privé accessible au public.

REFERENCES

(1) CPVP, Avis n° 17/2008 du 9 avril 2008, spéc. § 10, §21 (disponible sur https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_17_2008_0.pdf)

(2 Règlement général sur la protection des données ("RGPD") du 27 avril 2016 (disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679)
Groupe de travail "Article 29" sur la protection des données, GT 80 – *Document de travail sur la biométrie*, adopté le 1er août 2003 (disponible sur https://www.apda.ad/sites/default/files/2018-10/wp80_fr.pdf)

(3) Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. (disponible sur https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=2018073046).

(4) APD, Décision du Secrétariat Général 01/2019, 16 janvier 2019 (disponible sur https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/01_2019_SG.pdf).

JOACHIM PARMENTIER

belgium@lexing.network

BELGIUM

LEXING BELGIUM

Facial recognition: biometric data processing

▪ *Although it has not (yet) pronounced itself precisely on the issue of facial recognition, the Belgian Data Protection Authority ("DPA") provides insights into the processing of biometric data. The facial recognition process involves data that are linked to the individual's/data subject's own body (see article 4, 14° of the "GDPR").*

Opinion n°17/2008 of the DPA: authentication of persons

▪ *The Authority ("Privacy Commission," before December 2017) issued an opinion (1) on the processing of biometric data, solely for the purpose of authenticating individuals. This process thus allows the controller to verify that a person is who he or she claims to be (in the context of access control). In addition to this authentication function, facial recognition also makes it possible to identify individuals (finding a person in a crowd, for example).*

General data protection regulation and the Act on the protection of natural persons with regard to the processing of personal data, July 30th, 2018.

▪ *Even though this DPA opinion remains useful, it no longer reflects the current situation in this area. Indeed, since the enter into force of the GDPR, the processing of biometric data has been subject to a stricter legal framework:*

- *Article 9 of the GDPR (2): On the basis of this provision, biometric data are sensitive data. Therefore, the principle is that the processing of such data should be prohibited. Nevertheless, paragraph 2 of that provision provides that the controller may process these data in several cases. It is interesting to note that the legal basis relating to the "legitimate interest" of the controller is not among the exceptions listed in § 2.*
- *Article 9 of the Act of July 30th, 2018 (3): On the basis of Article 9, § 4 of the GDPR, the Belgian legislator added a condition to the processing of biometric data. Article 9 of the said Act provides that the controller must take "additional measures" when biometric data are processed. These measures, of which there are three, consist of precisely identifying the persons who have access to biometric data, communicating the list of their identity to the DPA and ensuring that these persons are bound by a legal obligation or an equivalent contractual provision, to respect the confidentiality of these data.*

Mandatory data protection impact assessment

▪ *Eventually, the DPA has issued an Opinion (4) in which it lists the data processing operations for which an impact assessment is mandatory. According to this list, such analysis must be carried out when the processing uses biometric data for the unique identification of data subjects in a public or private place accessible to the public.*

REFERENCES

(1) Belgian Privacy Commission, Opinion n°17/2008, April 9th, 2008, especially § 10, §21. (https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_17_2008_0.pdf)

(2) General data protection Regulation, April 27th, 2016 (https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679)
"Article 29" data Protection Working Party, WP 80 – Working document on biometrics, August 1st, 2003 (https://www.apda.ad/sites/default/files/2018-10/wp80_fr.pdf)

(3) Act on the protection of natural persons with regard to the processing of personal data, July 30th, 2018 (https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=2018073046).

(4) DPA, General Affairs' decision, 01/2019, January 16th, 2019 (https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/01_2019_SG.pdf).

JOACHIM PARMENTIER

belgium@lexing.network

▪ La reconnaissance faciale : un choix de société ? En France comme dans le reste de l'Europe, la reconnaissance faciale met en tension les droits fondamentaux. Selon la Cnil, elle appelle des choix politiques : sur le rôle dévolu à la technologie, sur ses effets sur les libertés fondamentales des individus et sur la place de l'humain à l'ère numérique (1).

(1) Reconnaissance faciale : pour un débat à la hauteur des enjeux, Cnil, 15 novembre 2019

▪ A l'automne 2019, Cédric O, secrétaire d'Etat au Numérique, déclarait au Monde à propos de la reconnaissance faciale : « *Comme souvent, la technologie est en avance sur la régulation. Aujourd'hui, la reconnaissance faciale entre dans nos vies sans que son cadre d'utilisation n'ait encore été clarifié. Elle offre de nouveaux usages, de nouvelles opportunités, mais surtout crée beaucoup de fantasmes du fait de l'absence d'un vrai débat citoyen sur les lignes rouges que nous souhaitons collectivement poser* » (2).

(2) Cédric O : « Expérimenter la reconnaissance faciale est nécessaire pour que nos industriels progressent », Le Monde du 14 octobre 2019

▪ Tout est dit à propos de cette technologie actuellement au centre de toutes les attentions et qui illustre plus que toute autre la tension qui naît lorsqu'un processus de décision quel qu'il soit, initialement confié à un humain – ici la reconnaissance à des fins d'authentification, d'identification, de surveillance, de protection… - se trouve en tout ou partie automatisée.

▪ Dans un tel cadre, les droits fondamentaux des personnes doivent conserver toute leur intensité et la dignité être préservée, tandis que l'atteinte à la vie privée
– si elle ne peut être évitée – doit être respectueuse du principe de proportionnalité.

▪ C'est ce qu'a rappelé la Cnil à l'occasion d'expérimentations prévoyant le recours à la reconnaissance faciale à l'entrée de deux lycées marseillais et niçois, l'autorité de régulation considérant en l'espèce que « *ce dispositif concernant des élèves, pour la plupart mineurs, dans le seul but de fluidifier et de sécuriser les accès n'apparaissait ni nécessaire, ni proportionné pour atteindre ces finalités* » (3).

(3) Cnil, Séance plénière du 17 octobre 2019

▪ Un mois plus tard, la Cnil appelait à un débat ne devant pas se résumer à un examen technique des potentialités d'usage et de l'efficacité de cette technologie, ce débat ne pouvant davantage « *avoir pour simple objectif de savoir comment rendre acceptable par les citoyens une technologie dont la nécessité s'imposerait de manière évidente. Car tel n'est pas le cas : le sujet est complexe et mérite un débat lucide et approfondi. C'est donc l'objet du débat que de déterminer dans*
quels cas la reconnaissance faciale est nécessaire dans notre société démocratique, et ceux dans lesquels elle ne l'est pas ».

Une technologie aux progrès vertigineux

▪ On le sait, la reconnaissance faciale, qui n'en était qu'à ses débuts, il y a trois ans à peine, a fait depuis l'objet de progrès spectaculaires, notamment grâce aux technologies chinoise et américaine, avec le développement de capteurs 3D.

▪ En Chine, on pense évidemment au *« crédit social »* qui interpelle tant notre culture européenne, en ce qu'il consiste, sur la base de la reconnaissance faciale,

à noter les habitants en fonction de leur comportement, même si, contrairement à un lieu commun, la Chine ne se jette pas dans la course du progrès en renonçant à toute éthique (4).

(4) Gaspard Koenig, La fin de l'individu, Editions de l'Observatoire, 2019.

▪ Dans ce domaine, les Etats Unis ne sont pas en reste : des centres commerciaux où l'IA s'invite de plus en plus, peuvent d'ores et déjà connaître le nom des clients lorsqu'ils pénètrent dans leur enceinte, regarder ce qu'ils achètent et sur la base de l'expression de leur visage, leur envoyer des promotions pour encourager à revenir.

Un cadre juridique en gestation

▪ En France, les technologies de reconnaissance faciale sont encadrées par la loi Informatique et libertés.

▪ Elles appartiennent à la catégorie des systèmes biométriques qui, lorsqu'ils ne sont pas justifiés par l'intérêt public, ne peuvent être mis en œuvre sans le consentement des personnes concernées dont les données biométriques sont utilisées.

▪ La liberté du consentement suppose que la personne concernée dispose d'un choix réel et non contraint*, « entendu comme la manifestation de leur volonté libre, spécifique et éclairée »* (5).

(5) Cnil, Délib. 2018-012 du 18 janvier 2018).

▪ Au sein de l'Union européenne, l'utilisation de tels dispositifs faisant intervenir des données biométriques est encadrée par le Règlement général sur la protection des données (RGPD).

▪ La Commission européenne prépare de son côté un règlement qui autorisera les citoyens de l'Union européenne à contrôler l'utilisation de leurs données de reconnaissance faciale. L'objectif : restreindre l'utilisation croissante de cette technologie par les acteurs économiques et les autorités avec en filigrane la volonté de s'assurer que le recours à l'IA dans ce domaine se fasse avec le consentement des citoyens. Le texte européen, s'il voit le jour, constituera, à n'en pas douter, une première traduction concrète d'un véritable droit de l'IA que nous appelons de nos vœux. Un droit encadrant l'IA qui devra nécessairement reposer sur le principe *« Ethics by design »* centré sur l'éthique et l'humain (6).

(6) Cf. J. Bensoussan, J-F Henrotte, « Legal Aspects of Artificial Intelligence », LexisNexis UIA, 2019 ; A. & J. Bensoussan, « Robot, IA et Droit », Bruylant, 2019) ; Alain Bensoussan, « Reconnaissance faciale aux abords des lycées, les précisions de la Cnil », DigitalMag n°258 p.42-43 décembre 2019 ; Reconnaissance faciale : quels enjeux pour quel cadre juridique ? Ibid, n°257, novembre 2019, p.34

▪ C'est aussi ce nouvel écosystème juridique qui participe à maintenir l'intelligence artificielle au service du bien commun.

ALAIN BENSOUSSAN

france@lexing.network

▪ *Facial recognition: a societal choice? In France, as in the rest of Europe, facial recognition puts fundamental rights at odds. According to the CNIL, facial recognition calls for political choices to be made: on the role we give this technology, on how it affects the fundamental freedoms of individuals, and on what our place is in the digital age (1).*

(1) *Facial recognition: for a debate living up to the challenges, CNIL, 19 December 2019*

▪ *In the autumn of 2019, Cédric O, Minister of State for the Digital Sector, was interview by the newspaper* Le Monde *about facial recognition and said "As is often the case, technology is ahead of regulation. Today, facial recognition is entering our lives without its framework of use having yet been clarified. It offers new uses, new opportunities, but above all creates a lot of fantasies because of the lack of a real citizen debate on the red lines we collectively wish to draw" (2).*

(2) *Cédric O: "Expérimenter la reconnaissance faciale est nécessaire pour que nos industriels progressent", Le Monde, 14 October 2019*

▪ *That says it all about this technology which is currently the focus of attention and which illustrates better than anything else the tension that arises when a decision-making process of any kind, initially entrusted to a human being (here, recognition for authentication, identification, surveillance, or protection purposes) is wholly or partly automated.*

▪ *In such a framework, the fundamental rights of individuals must apply to their full extent and dignity must be preserved, while the infringement of privacy — if it cannot be avoided — must respect the principle of proportionality.*

▪ *These points were emphasised by the CNIL. In reviewing trials involving the use of facial recognition at the entrance to two secondary schools in Marseille and Nice, the French supervisory authority said "*this system concerning pupils, most of whom are minors, with the sole aim of making access more fluid and secure did not appear to be necessary or proportionate to achieve these aims *(3)."*

(3) *CNIL, plenary session of 17 October 2019*

▪ *A month later, the CNIL called for a debate that should not be limited to a technical consideration of the potential uses and effectiveness of this technology. Nor should it "*solely be aimed at finding out how to make acceptable to citizens a technology which would be necessary. It is indeed not the case: it's a complex issue, and one that warrants a lucid and in-depth debate. The purpose of this debate is therefore to determine in which cases facial recognition is necessary in a democratic society, and in which cases it is not."

A technology that is making dizzying progress

▪ *Facial recognition, which was only in its infancy just three years ago, has since made spectacular progress, thanks in particular to Chinese and American technology, with the development of 3D sensors.*

▪ *In China, we are obviously thinking of the 'social credit', which consists in using facial recognition to rate inhabitants according to their behaviour; this clashes with our European culture, even if, contrary to a widespread belief, China does not throw itself into the race for progress by abandoning all ethics (4).*

(4) *Gaspard Koenig, La fin de l'individu, Editions de l'Observatoire, 2019.*

▪ *The United States is also not to be outdone: shopping malls are increasingly using AI and can already know the names of customers when they enter their premises, look at what they are buying and, on the basis of their facial expressions, send them promotions to encourage them to come back.*

A legal framework in the making

▪ *In France, facial recognition technologies are governed by the Data Protection Act.*

▪ *They belong to the category of biometric systems which, when not justified by the public interest, cannot be implemented without the consent of the data subjects whose biometric data are used.*

▪ *The freedom of consent presupposes that the data subject has a real and uncoerced choice, "*understood as the freely given, specific and informed indication of their wishes *(5)."*

▪ *In the European Union, the use of devices involving biometric data is regulated by the General Data Protection Regulation (GDPR).*

▪ *The European Commission is also preparing a regulation that will give European Union citizens control over the use of their facial recognition data. The aim is to restrict the increasing use of this technology by economic players and authorities, with the underlying desire to ensure that the use of AI in this area is done with the consent of citizens. The European text, if it were to be adopted eventually, will undoubtedly be the first concrete translation of a genuine AI law that we are calling for. A law governing AI which will necessarily have to be based on the principle of 'Ethics by design' centred on ethics and human beings (6).*

▪ *This new legal ecosystem will also contribute to maintaining an artificial intelligence that serves the common good.*

(5) Cnil, Deliberation 2018-012 of 18 January 2018.

(6) See J. Bensoussan, J-F Henrotte, "Legal Aspects of Artificial Intelligence", LexisNexis UIA, 2019; A. & J. Bensoussan, "Robot, IA et Droit", Bruylant, 2019); Alain Bensoussan, "Reconnaissance faciale aux abords des lycées, les précisions de la Cnil", DigitalMag n° 258 p.42-43 December 2019; "Reconnaissance faciale : quels enjeux pour quel cadre juridique ?" Ibid, n°257, November 2019, p.34

ALAIN BENSOUSSAN

france@lexing.network

GRÈCE

BALLAS, PELECANOS & ASSOCIATES L.P.C.

Le principe général applicable au traitement des données biométriques

▪ En Grèce, le principe général applicable au traitement des données biométriques résulte principalement de la jurisprudence de l'autorité de protection des données et peut se résumer ainsi : l'utilisation de systèmes biométriques peut être autorisée, dans le respect du principe de proportionnalité (1), afin de répondre à des exigences de sécurité élevées relatives au contrôle d'accès (identification et authentification) à certaines zones physiques.

▪ Ces zones peuvent être des infrastructures critiques, comme le réseau de métro ou les aéroports (1), ou bien des systèmes informatiques, tels que des applications militaires ou bancaires critiques (2).

La biométrie dans le cadre des relations de travail

▪ L'utilisation de méthodes biométriques dans le cadre des relations de travail à des fins d'identification et de contrôle d'accès ne peut être autorisée que lorsque cela est nécessaire en raison d'exigences de sécurité particulières (laboratoires à haut risque ou installations de haute sécurité) à condition qu'il n'existe pas d'autres moyens plus respectueux de la vie privée pour atteindre cet objectif.

▪ Par exemple, l'autorité grecque de protection des données a autorisé un fournisseur de services de certification de signature électronique à utiliser un système biométrique, afin de contrôler l'accès de son personnel à certaines zones de haute sécurité (3).

▪ Cependant, dans la majorité des cas, l'autorité de protection des données estime que l'utilisation de systèmes et de méthodes biométriques est manifestement disproportionnée au regard des risques qu'elle présente pour la protection des données, inappropriée et contraire aux règles et principes applicables en matière de protection des données (4).

REFERENCES

(1) Décision 9/2003 de l'Autorité hellénique de protection des données sur l'utilisation de la forme de la main pour contrôler l'accès des employés aux installations à haut risque du métro d'Athènes ; Décisions 39/2004 et 31/2010 de l'Autorité hellénique de protection des données sur l'utilisation de systèmes biométriques à l'aéroport international d'Athènes et à l'aéroport de Thessalonique.

(2) Décision 52/2008 de l'Autorité hellénique de protection des données.

(3) Décision 56/2009 de l'Autorité hellénique de protection des données.

(4) Décision 59/2005 de l'Autorité hellénique de protection des données rejetant l'installation d'un système biométrique pilote pour le contrôle d'accès aux installations sportives ; Décision 62/2007 de l'Autorité hellénique de protection des données rejetant l'installation d'un système biométrique pour le contrôle d'accès aux zones de travail ; Décision 245/9/2000 de l'Autorité hellénique de protection des données qui a jugé illégale l'utilisation d'empreintes digitales par les autorités municipales pour contrôler l'accès des employés aux zones de travail.

GEORGE A. BALLAS
&
THEODORE KONSTANTAKOPOULOS

greece@lexing.network

The general rule

▪ *The general principle on the issue of processing of biometric data has been primarily formulated by the case law produced by the Hellenic Data Protection Authority, according to which, use of biometric systems can be permitted, in compliance with the principle of proportionality (1), in order to meet high security requirements for access control (i.e. identification and authentication purposes) to certain physical areas.*

▪ *Such areas may be critical infrastructures, like the metro system or airports (1), or computer systems, e.g. critical military or banking applications (2).*

Biometrics in the context of employment

▪ *The use of biometric methods in the context of employment for identification and access control purposes can be permissible only when this is required due to special safety requirements. This, for instance, would be the case of high-risk laboratories or high security facilities and where, at the same time, there is no other, less privacy intrusive means to achieve said purpose.*

▪ *For example, the Hellenic Data Protection Authority has permitted the use of a biometric system by a provider of electronic signature certification services, in order to control personnel access to certain high security areas (3).*

▪ *There is however a majority of cases, where the Hellenic Data Protection Authority has deemed that the use of biometric systems and methods is clearly disproportionate to the data privacy risks posed and has found such use to be inappropriate and in breach of applicable data protection rules and principles (4).*

REFERENCES

(1) Decision 9/2003 of the Hellenic Data Protection Authority on the use of the shape of the hand to control employees' access to high-risk facilities of the Athens Metro, the rapid-transit system in Athens); Decision 39/2004 and Decision 31/2010 of the Hellenic Data Protection Authority on the use of biometric systems at the Athens International Airport and the Thessaloniki Airport.

(2) Decision 52/2008 of the Hellenic Data Protection Authority.

(3) Decision 56/2009 of the Hellenic Data Protection Authority.

(4) Decision 59/2005 of the Hellenic Data Protection Authority rejecting the installation of a pilot biometric system for access control to sports facilities; Decision 62/2007 of the Hellenic Data Protection Authority rejecting the installation of a biometric system for access control to working areas; Decision 245/9/2000 of the Hellenic Data Protection Authority which found illegal the use of fingerprints by Municipal Authority to control access of employees to working areas.

GEORGE A. BALLAS
&
THEODORE
KONSTANTAKOPOULOS

greece@
lexing.network

▪ Nouvelles technologies biométriques : analyse vidéo et analyse radio. Le présent article s'intéresse aux enjeux soulevés par les nouvelles méthodes d'analyse de données biométriques ainsi qu'à leurs conséquences potentielles dans le cadre du RGPD. Il se penche également sur l'impact de l'analyse vidéo et de l'analyse radio, et aborde la détection sans fil, la radio-biométrie ainsi que la reconnaissance sans fil des émotions.

▪ Les données biométriques font partie des catégories particulières de données à caractère personnel dont le traitement est interdit par l'article 9 du RGPD, en dehors des exceptions prévues à l'article 9.2.

▪ Les technologies décrites ci-dessous utilisent des données biométriques pour offrir une meilleure localisation des consommateurs et des individus, souvent sans tenir compte des risques qui peuvent découler de l'utilisation et du traitement de ces données. Deux domaines d'analyse susceptibles de créer des risques pour les données à caractère personnel qu'ils traitent seront plus particulièrement étudiés : l'analyse vidéo et l'analyse radio.

▪ L'analyse vidéo consiste à analyser des données à caractère personnel enregistrées au moyen des technologies vidéo. Les objectifs poursuivis sont divers, allant de la sécurité à l'analyse statistique, en passant par le marketing ou encore le profilage de clients. Les technologies d'analyse vidéo existent depuis un certain temps déjà et ouvrent de nouvelles possibilités par rapport aux technologies de vidéosurveillance traditionnelles. De plus en plus répandue, l'analyse vidéo a fait l'objet de lignes directrices du CEPD, publiées le 20 janvier 2020 (« les lignes directrices »). (1)

▪ Dans ses lignes directrices, le CEPD procède à une analyse approfondie des technologies d'analyse vidéo, considérées dangereuses en raison de la nature potentiellement intrusive des traitements qu'elles peuvent permettre. Le CEPD se penche particulièrement sur les nombreuses problématiques soulevées par la reconnaissance faciale. A cet égard, il rappelle qu'il faut avant tout identifier si des données biométriques sont traitées et les types de données traités. Il est en effet important de distinguer les techniques qui ne traitent pas nécessairement des données biométriques (comme la détection d'objets ou d'événements) des techniques de reconnaissance faciale, qui requièrent la création un gabarit biométrique des individus observés et qui, à ce titre, réalisent bien des traitements de données biométriques. Autre point de vigilance : la base juridique du traitement. Dans le cas de la reconnaissance faciale, la base juridique devrait être (dans la grande majorité des cas) le consentement de la personne concernée, comme le prévoit l'article 9.2 du RGPD. A défaut, il est nécessaire de veiller au respect du principe de licéité et de loyauté du traitement (art. 5.1 (a) du RGPD).

▪ La reconnaissance faciale est très utilisée dans les lieux publics fréquentés par un grand nombre de personnes (centres commerciaux, stades et arènes lors d'événements sportifs, magasins) afin, notamment, de personnaliser les publicités et les promotions commerciales. Dans de tels cas, toute personne utilisant un système de reconnaissance faciale est tenue (a) d'obtenir le consentement valable

REFERENCES

(1) CEPD, Lignes directrices sur le traitement de données à caractère personnel par des appareils vidéo 3/2019 (en anglais uniquement), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

(2) « Différents types d'analyse, appelées analyses radio, qui peuvent déchiffrer les ondes radio pour révéler les activités ayant lieu autour de nous, sur la base des informations sur l'état du canal de transmission (CSI) sans fil, peuvent être développés pour rendre possibles de nombreuses applications de pointe de l'IdO envisagées depuis longtemps mais jamais réalisées. » The Promise of Radio Analytics: A Future Paradigm of Wireless Positioning, Tracking, and Sensing, IEEE Signal Processing Magazine, Maggio 2018, B. Wang, C. Chen, Q. Xu, F. Zhang, (https://ieeexplore.ieee.org/document/8350392).

(3) Beibei Wang, Qinyi Xu, Chen Chen, Feng Zhang, K.J. Ray Liu, infra, « Dans cette section, nous examinons un nouveau concept de radio-biométrie utilisant les informations sur l'état du canal de transmission (CSI) à trajets multiples, grâce auquel il est possible de procéder, de manière précise, à l'identification et à la vérification de personnes physiques au moyen d'appareils Wi-Fi commerciaux, même en présence de murs », p.72, sia WBA Wi-Fi Sensing Group, Wireless Broadband Alliance, Wi-Fi Sensing A New Technology Emerges, octobre 2019, « La détection haute résolution peut être utilisée afin de mesurer des données physiologiques et comportementales pour des applications de sécurité et médicales. Les mesures de données biométriques comprennent les battements de cœur et les fréquences respiratoires. Ces informations peuvent être utilisées pour surveiller les patients de manière passive et non invasive, [...] De plus, la détection haute résolution a des applications en matière de

de toutes les personnes concernées et (b) de donner à toute personne n'ayant pas donné son consentement préalable la possibilité d'entrer dans les locaux, par exemple en lui réservant des entrées spécifiques et en lui permettant d'emprunter des chemins alternatifs, tout en s'interdisant naturellement de traiter les données biométriques de cette personne.

▪ Autre technologie intéressante, le « wireless sensing ». Issue de l'analyse radio, cette technologie de détection sans fil utilise des données biométriques, pour l'instant à des fins non commerciales. L'analyse radio analyse les ondes radio, en particulier le Wi-Fi, pour comprendre et décrypter la réalité qui nous entoure. (2) Ses applications commerciales sont le traçage par Wi-Fi et le géolocalisation par Wi-Fi, où les signaux émis par un appareil sont analysés afin de collecter des informations sur son propriétaire telles que sa position, la fréquence de sa présence dans un lieu donné, les achats effectués, etc. Dans ce cas, c'est la présence d'un appareil émetteur d'ondes porté par une personne (smartphone, tablette, etc.) qui déclenche l'analyse et le traitement de données à caractère personnel.

▪ La détection sans fil, en revanche, permet d'obtenir des informations sur une personne indépendamment du fait que celle-ci ait un appareil en sa possession. En effet, pour obtenir des données, il suffit qu'un individu entre dans le champ d'un dispositif émettant un signal Wi-Fi (par exemple, les routeurs que nous avons à la maison ou au bureau). Pourront alors être analysés les micro variations de l'environnement causées par la présence d'objets et de personnes dans son champ d'ondes. En d'autres termes, il serait possible non seulement de cartographier des locaux, mais aussi de reconnaître et d'analyser des mouvements, des gestes et tout signe vital comme les battements de cœur, la fréquence respiratoire, etc. Cette technologie de détection sans fil est connue sous le nom de radio-biométrie (« radio biometrics »). (3)

▪ Dès lors lorsqu'elles sont utilisées pour identifier une personne de manière univoque, ces informations sont des données biométriques et sont soumises aux mêmes règles que celles indiquées précédemment pour la reconnaissance faciale. Or, la radio-biométrie peut être beaucoup plus intrusive que la reconnaissance faciale, dans la mesure où elle permettrait de recueillir, en temps réel, des informations sur les mouvements des personnes concernées dans une zone donnée, de cartographier cette zone et de savoir combien de personnes y sont présentes, de « lire » leurs signes vitaux et, au bout du compte, de recueillir des données biométriques sans qu'il soit nécessaire d'installer des dispositifs ad hoc (4).

▪ C'est évidemment très inquiétant, d'autant plus que des travaux de R&D en cours envisagent d'utiliser cette technologie pour comprendre et détecter les émotions d'individus (5) : cette technique, dite de reconnaissance d'émotions sans fil (« wireless emotion recognition »), poserait d'importantes questions en termes de protection des données à caractère personnel. Il suffit d'imaginer qu'elle soit appliquée aux innombrables appareils connectés (Alexa, Google Home etc.) déjà présents au sein des foyers : chacun de ces appareils pourrait intégrer cette nouvelle technologie instantanément, par mise à jour de son logiciel, et ainsi
recueillir et traiter des données dans ce but, à l'insu des personnes concernées.

sécurité, comme dans le cas des polygraphes », p. 15, https://wballiance.com/resource/wi-fi-sensing/.

(4) Beibei Wang, Qinyi Xu, Chen Chen, Feng Zhang, K.J. Ray Liu, infra, « nous examinons la manière d'atteindre une précision centimétrique avec les systèmes de géolocalisation en intérieur (IPS) sans fil, offrant offrir une capacité de type GPS (Global Positioning System) en intérieur, afin de suivre les humains ou tout objet dans un espace intérieur sans aucune infrastructure, pour autant que le Wi-Fi ou l'évolution à long terme (LTE) soient disponibles », p. 60.

(5) Pour les abus et détournements qui pourraient en résulter, cf. A. M. Khalili, Abdel-Hamid Soliman, Md Asaduzzaman, Alison Griffiths, Wi- Fi Sensing: Applications and Challenges, Cornell University, arXiv:1901.00715 [cs.HC], 28 mai 2019, « [l]e système transmet un signal sans fil et analyse les réflexions du corps de l'utilisateur pour reconnaître ses émotions telles que le bonheur, la tristesse, etc. La composante clé du système est un nouvel algorithme qui extrait les battements du cœur du signal sans fil avec une précision proche de celle des moniteurs d'électrocardiogramme (ECG). Les battements de cœur extraits sont ensuite utilisés pour extraire des caractéristiques liées aux émotions, puis ces caractéristiques sont utilisées dans un classificateur d'émotions à apprentissage automatique. Les chercheurs ont démontré que la précision de la reconnaissance des émotions est comparable à celle des systèmes de reconnaissance des émotions de pointe basés sur les moniteurs ECG. La précision de la classification des émotions est de 87% dans le système proposé et de 88,2% dans les systèmes basés sur l'ECG ».

ALFREDO ZALLONE

italy@lexing.network

New Biometric technologies: video analytics and radio analytics. What are the possible impacts of new methods of analysis of biometric data and what are the potential consequences under the GDPR? The impact of video analytics and radio analytics, with a brief overview on wireless sensing, radio biometrics and wireless emotion recognition.

- *Biometric data fall in the categories of personal data regulated under Article 9 of the GDPR, which states as general principle that their processing is forbidden, with the exceptions listed under Article 9.2.*

- *The technologies I shall examine use biometric data to offer a better localization of consumers and individuals, often without proper care of the potential risks that may derive from their use and processing. I shall specifically concentrate on two areas of analytics that may create risks for the personal data they process: Video Analytics and Radio Analytics.*

- *Video analytics consists of the analysis of personal data recorded with video technologies; the personal data are processed for several purposes: security, statistics, marketing, customer profiling, etc. The technologies of video analytics have been available for quite some time; they are used for very different purposes with respect to the traditional video-surveillance technologies. In addition, video analytics is getting quite common and the EDPB has dealt with this technology in the guidelines issued on January 20, 2020 ("the Guidelines"). (1)*

- *The Guidelines analyze thoroughly the technologies of video analytics, which it considers quite dangerous due to the potential intrusive nature of the processing that they can allow. Specific attention has been given in the Guidelines to facial recognition, which also poses several problems. The first problem derives from the need to understand if biometric data are being processed and what biometric data are being processed. In fact, it's important to distinguish techniques like object detection or event detection, that do not necessarily process biometric data, from techniques of facial recognition, which operate by creating a biometric template of the individuals observed, and as such process biometric data. Having established this difference, the second problem is to determine the correct legal basis to process these data; in the case of facial recognition the basis should be (in the vast majority of situation) the consent of the data subject, as established by Article 9.2 of the GDPR. This implies (third problem) the need to comply with the principle of lawfulness and fairness of the processing (Article 5.1 (a) of the GDPR) for processing biometric data of data subjects who do not consent to this processing.*

- *A typical example of the use of facial recognition is in the systems used in public areas attended by large number of people (shopping malls, stadiums and arenas in sport events, shops) where these systems are used to personalize commercial ads and promotions. In such cases anyone using a facial recognition system should: (a) obtain a valid consent from all data subjects and (b) in any case give the possibility to enter the premises to anyone who has not given her/his prior consent, for*

REFERENCES

(1) EDPB, Guidelines 3/2019 on processing of personal data through video devices, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

(2) "[V]arious types of analytics, referred to as radio analytics, that can decipher the radio waves to reveal the activities around us, based on the wireless channel state information (CSI), can be developed to enable many cutting-edge IoT applications envisioned for a long time but never achieved." The Promise of Radio Analytics: A Future Paradigm of Wireless Positioning, Tracking, and Sensing, IEEE Signal Processing Magazine, Maggio 2018, B. Wang, C. Chen, Q. Xu, F. Zhang, (https://ieeexplore.ieee.org/document/8350392).

(3) Beibei Wang, Qinyi Xu, Chen Chen, Feng Zhang, K.J. Ray Liu, infra, "In this section, we discuss a novel concept of radio biometrics utilizing the multipath CSI, based on which accurate human identification and verification can be implemented with commercial Wi-Fi devices, even in a through-the-wall setting", p.72, sia WBA Wi-Fi Sensing Group, Wireless Broadband Alliance, Wi-Fi Sensing A New Technology Emerges, October 2019, "High-resolution sensing can be utilized to measure physiological and behavioral data for security and medical applications. Biometric data measurements include heartbeat and respiration rates. This information can be used for monitoring patients in a noninvasive and passive manner, […] Additionally, high-resolution sensing has security applications, such as in the case of polygraphs", p. 15, https://wballiance.com/resource/wi-fi-sensing/.

(4) Beibei Wang, Qinyi Xu, Chen Chen, Feng Zhang, K.J. Ray Liu, infra, "we discuss how to achieve centimeter accuracy in wireless indoor positioning systems (IPSs)

example by dedicating specific entrances and allowing alternative paths; obviously without processing the biometric data of any data subject who has not consented to the processing.

▪ *The other technology I want to briefly discuss is a branch of radio analytics called wireless sensing, a system using biometric data, presently not yet used for commercial purposes. Radio analytics analyzes radio waves, in particular wi-fi, to understand and "decrypt" the reality surrounding us. (2) Its commercial applications are wi-fi tracking and wi-fi positioning, technologies that analyze the signals emitted by device in order to collect information on its owner such as position, frequency of presence in a given place, purchases made, etc. The presence of a device carried by a data subject (smartphone, tablet, etc.) that emits waves triggers the analysis and processing of personal data.*

▪ *Wireless sensing on the other hand is a technology that allows to obtain information on a data subject independently from the fact that such subjects carries a device; in fact, in order to obtain the data to be analyzed, it is enough that the data subject to enter a wi-fi field. If there is a device emitting a wi-fi signal (like the routers we have home or in our offices) this technology is capable of analyzing micro variations of the environment caused to the presence of objects and persons within its wave field. In other words, this technology could not only allow to map premises, but it could recognize and analyze movements, gestures and any vital sign like hart-beats, breath frequency, etc. This wireless sensing technology is known as radio biometrics. (3)*

▪ *This kind of information, when used to univocally identify a data subject, do certainly fall in the category of biometric data and would require the same discipline as previously indicated for facial recognition. On the other hand it is clear that this technology may be significantly more intrusive as compared to facial recognition, in that it would allow to collect in real-time information on the movements of data subjects in any given area, to map such area and to know how many people are present, to "read" their vital signs, in the final analysis to collect biometric data without the need to install ad-hoc devices.(4)*

▪ *This is obviously very disturbing, the more so if one thinks that R&D is on-going in this area, with the aim to use this technology to understand and sense the emotions of the data subjects (5): this additional development of this technology, code-named as wireless emotion recognition, would raise very significant issues related to the protection of personal data. The more so if one thinks how many devices like Alexa or Google Home have been sold and deployed: anyone of such devices could be upgraded in no time with this new function at any new, periodical SW update, and this could happen without the data subject being aware of this new function as well as of this processing.*

that can offer an indoor Global Positioning System (GPS)-like capability to track human or any indoor objects without any infrastructure, as long as Wi-Fi or long-term evolution (LTE) is available", p. 60

(5) For possible misuses see A. M. Khalili, Abdel-Hamid Soliman, Md Asaduzzaman, Alison Griffiths, Wi-Fi Sensing: Applications and Challenges, Cornell University, arXiv:1901.00715 [cs.HC], 28 May 2019, "[t]he system transmits a wireless signal and analyses the reflections from the user body to recognise his emotions such as happiness, sadness, etc. The key building block of the system is a new algorithm that extracts the heartbeats from the wireless signal at an accuracy close to Electrocardiogram (ECG) monitors. The extracted heartbeats are then used to extract features related to emotions, then these features are used in a machine learning emotion classifier. The researchers demonstrated that the emotion recognition accuracy is comparable with the state of the art emotion recognition systems based on ECG monitors. The accuracy of emotion classification is 87% in the proposed system and 88.2% in the ECG based systems".

ALFREDO ZALLONE

italy@
lexing.network

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.	Jean-François De Rico	+1 (418) 650 7000	canada@lexing.network
Chine *China*	Jade & Fountain PRC Lawyers	Jun Yang	+86 21 6235 1488	china@lexing.network
Costa Rica *Costa Rica*	Lexing Costa Rica	Gabriel Lizama	+506 2253-1726	costa-rica@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
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
Israël *Israel*	Appelfeld & Co	Ilanit Appelfeld	+ 972 3 60 98 099	israel@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
Luxembourg *Luxembourg*	Emmanuelle Ragot	Emmanuelle Ragot	:(+352) 661 84 42 50	luxembourg@lexing.network
Maroc *Morocco*	Fayçal Elkhatib et Associés S.C.P.A	Hatim Elkhatib	+212 5 39 94 05 25	morocco@lexing.network
Mexique *Mexico*	Carpio, Ochoa & Martínez Abogados	Enrique Ochoa De González 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/