PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Dossier d'information du citoyen et guide pour les personnes vulnérables

Cette œuvre est protégée par une licence [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](#).

Ce projet a reçu un financement du programme de recherche et d'innovation Horizon 2020 de l'Union européenne dans le cadre de la convention de subvention n° 788039. Il ne reflète que le point de vue de l'auteur et l'Agence n'est pas responsable de l'usage qui pourrait être fait des informations qu'il contient.

Informations sur le projet

Titre du projet	Approches participatives pour un nouveau cadre éthique et juridique des TIC
Acronyme du projet	PANELFIT
Numéro de la convention de subvention	788039
Coordinateur de projet	UPV/EHU

Informations sur les documents

Numéro du livrable	D5.5
Titre du document	Dossier d'information pour les citoyens
Version du document	3.0
Date du document	22 avril 2022
Paquet de travail	WP5
Tâche	Tâche 5.7
Responsable du document	OBCT / ECSA
Licence de droit d'auteur	Licence internationale Creative Commons Attribution-NonCommercial-NoDerivatives 4.0.
Niveau de diffusion	PU = Accès PUBLIC non restreint - Projet européen
Échéance contractuelle	2021-08-31 (Mois 34)

Partenaires du projet impliqués dans le document

Non.	Nom de l'organisation	Acronyme
1	Université du Pays basque / Euskal Herriko Unibertsitatea	UPV/EHU
7	Association européenne des sciences citoyennes	ECSA
8	Réseau européen des comités d'éthique de la recherche	EUREC
9	Institut de Ciències del Mar (Consejo Superior de Investigaciones Científic)	ICM-CSIC
10	OBC Transeuropa	OBCT

Historique des documents

Statut	Version	Date	Auteur(s)	Révisé par
Draft	V1.0	21.7.2021	Tim Woods (ECSA)	
Modifier	V1.1	22.7.2021		Iñigo de Miguel Beriain (UPV/EHU)
Modifier	V1.2	18.8.2021		Federico Caruso (OBCT)
Final	V2.0	19.8.2021		
Final	V3.1	31.8.2021		Roberta Monachello (UE)
Final	V4.0	08.04.2022		Carolina Doran (ECSA), Federico Caruso (OBCT), Johann Cas (ÖAW) et Alessandro Ortalda (VUB)

Avertissement : Le contenu de cette publication relève de la seule responsabilité du consortium PANELFIT et ne reflète pas nécessairement l'opinion de l'Union européenne.

Table des matières

TIC, données et personnes vulnérables : un guide pour les citoyens 4
À propos de ce guide 5
Glossaire des termes clés 6
Quelles sont les questions éthiques et juridiques liées aux TIC ? 8
Qui est vulnérable ? 10
Comment les questions éthiques et juridiques liées aux TIC affectent-elles les personnes vulnérables ? 14
Que pouvez-vous faire ? 25
Remerciements 33
Dossiers thématiques 35
1. Commercialisation des données : opérateurs téléphoniques et données personnelles 35
2. La stratégie européenne de cybersécurité 44
3. Déséquilibres de pouvoir et liberté de consentement : La forteresse numérique qu'est l'Europe 59

TIC, données et personnes vulnérables : un guide pour les citoyens

Avis de non-responsabilité

Ce projet a été financé par le programme de recherche et d'innovation Horizon 2020 de l'Union européenne dans le cadre de la convention de subvention n° 788039. Ce document ne reflète que le point de vue de l'auteur et l'Agence n'est pas responsable de l'usage qui pourrait être fait des informations qu'il contient.

Citation

Consortium PANELFIT (2021) *TIC, données et personnes vulnérables : un guide pour les citoyens*. UPV-EHU, Bilbao.

À propos de ce guide

TIC, données à caractère personnel, droits numériques, RGPD, confidentialité des données, sécurité en ligne ; ces termes, et les concepts qui les sous-tendent, sont de plus en plus courants dans nos vies. Certains d'entre nous les connaissent peut-être, mais d'autres sont moins conscients du rôle croissant des TIC et des données dans nos vies - et des risques potentiels que cela engendre.

Dans ce guide, nous utilisons le terme "citoyen" pour désigner toutes les personnes qui sont des résidents européens, quelle que soit leur nationalité, ou dont les droits relèvent de la juridiction européenne, même si ce n'est que temporairement.

Ces risques sont encore plus prononcés pour les groupes vulnérables de la société. Les personnes peuvent être vulnérables de différentes manières, qui se recoupent souvent, ce qui les désavantage par rapport à la majorité des citoyens (le tableau 3 présente quelques-unes des nombreuses formes et causes de vulnérabilité). Par conséquent, les personnes vulnérables ont besoin d'un soutien accru pour naviguer dans le monde numérique et pour s'assurer qu'elles sont en mesure d'exercer leurs droits. Ce guide explique où trouver un tel soutien et répond également aux questions suivantes :

- Quels sont les principaux problèmes éthiques et juridiques liés aux TIC pour les citoyens vulnérables ?
- Qui est vulnérable en Europe ?
- Comment les questions relatives aux TIC affectent-elles les personnes vulnérables en particulier ?

Ce guide est une ressource pour les membres de groupes vulnérables, les personnes qui travaillent avec des groupes vulnérables et les citoyens en général. Il est également utile pour les "responsables du traitement des données"[5] qui collectent des données sur les citoyens vulnérables. Bien que centré sur les citoyens européens, il peut intéresser des personnes d'autres régions du monde.

Il fait partie du dossier d'information des citoyens produit par le projet PANELFIT, et est disponible en anglais, français, allemand, italien et espagnol. Vous êtes invités à traduire ce guide dans d'autres langues. Veuillez nous envoyer un lien vers les versions en ligne dans d'autres langues, afin que nous puissions les ajouter au site web du projet.

Glossaire des termes clés

Le tableau 1 explique certains des termes clés utilisés dans ce guide. Il ne s'agit pas du "dernier mot" sur ces termes, mais d'une définition utile pour ceux qui ne connaissent pas la terminologie relative aux TIC, aux données et aux groupes vulnérables.

Tableau 1. Termes clés pour comprendre les TIC, les données et les groupes vulnérables

Cybersécurité	Il s'agit du degré de protection des données et des informations privées en ligne, c'est-à-dire de leur protection contre le piratage, le vol ou la publication sans autorisation.
Commercialisation des données	Il s'agit de traiter des données concernant des personnes ou des groupes dans le but de gagner de l'argent, par exemple par le biais de publicités en ligne ciblées ou en les revendant à d'autres.
Responsable du traitement des données	Un responsable du traitement des données est toute personne qui obtient des données, y compris des données à caractère personnel, pour les utiliser dans un but précis. Il peut s'agir d'une entreprise, d'une organisation, d'un gouvernement ou d'une autorité locale, d'un organisme public (par exemple, une école ou un hôpital) ou d'un institut de recherche, entre autres.
Gestion des données	La gestion des données couvre l'ensemble du cycle de vie du traitement des données : collecte, utilisation, stockage, partage et suppression. Elle fait également référence au fait que la personne qui collecte vos données (le responsable du traitement) doit contrôler l'usage qui est fait de ces données et qui peut les utiliser.
Protection des données	Rien ne doit arriver à vos données personnelles à moins que vous n'en ayez donné l'autorisation. Les responsables du traitement des données sont tenus, en vertu de la législation européenne, de mettre en place des mesures pour garantir que les données sont stockées de manière sûre et confidentielle. Vos données ne doivent pas être partagées ou rendues publiques, sauf si vous y avez consenti.
Personne concernée	La personne dont les données personnelles sont collectées et utilisées par le responsable du traitement.

Utilisation et réutilisation des données	Lorsqu'ils vous demandent vos données, les responsables du traitement doivent vous expliquer les finalités pour lesquelles elles seront utilisées (par exemple, un recensement, un projet de recherche). Si eux-mêmes, ou un tiers, souhaitent utiliser vos données à d'autres fins - ce que l'on appelle la réutilisation des données - ils doivent vous demander à nouveau votre consentement. Ils ne peuvent pas supposer que vous êtes d'accord pour que vos données soient réutilisées.
La fracture numérique	Il s'agit de l'écart entre les personnes qui peuvent bénéficier de la technologie (par exemple, les TIC, internet) et celles qui ne le peuvent pas. Ce phénomène prend de plus en plus d'importance, car de plus en plus d'aspects de notre vie sont partiellement ou entièrement en ligne (par exemple, l'éducation, les soins de santé, la banque, les achats). Ceux qui n'ont qu'un accès limité ou nul aux services numériques risquent d'être "laissés pour compte".
Alphabétisation numérique	Parfois appelée "alphabétisation aux TIC", elle désigne la capacité d'une personne à trouver, évaluer et communiquer des informations sur des plateformes et des dispositifs numériques.
Droits numériques	Cela fait référence aux lois et procédures (par exemple, le RGPD) qui sont en place pour protéger nos droits dans le monde numérique. Ces droits comprennent, entre autres, le droit à la vie privée et le droit de retirer son consentement à l'utilisation des données.
Discrimination	La discrimination consiste à établir des distinctions injustifiées entre des personnes, sur la base de perceptions concernant ce groupe ou la (les) catégorie(s) à laquelle (auxquelles) elles appartiennent ; par exemple, leur race, leur sexe, leur âge, leur religion ou leur orientation sexuelle, entre autres.
RGPD	Le règlement général sur la protection des données réglemente la manière dont les données personnelles des citoyens européens sont gérées. En fait, il définit les lois par lesquelles vos données à caractère personnel sont protégées et gardées privées.
TIC	Les technologies de l'information et de la communication comprennent toutes les formes de technologies utilisées pour la communication, telles qu'internet, les téléphones mobiles et les smartphones, les ordinateurs, les réseaux de médias sociaux, les outils de vidéoconférence, et bien d'autres encore.
Consentement éclairé	En ce qui concerne les données et les TIC, il s'agit d'informer la personne concernée et de lui demander l'autorisation d'utiliser ses données personnelles d'une manière spécifique - ce qui doit être fait avant de collecter ou d'utiliser ses données.

Données à caractère personnel	Les données à caractère personnel sont tout ce qui vous concerne en tant qu'individu : votre nom, votre âge ou votre adresse, par exemple. Dans le monde numérique, elles peuvent également inclure vos centres d'intérêts, vos habitudes et vos préférences, par exemple les pages que vous "aimez" sur les réseaux sociaux, les sites web que vous visitez pour acheter des articles, les vidéos YouTube que vous avez regardées, et bien d'autres encore.
Vie privée	En ce qui concerne les TIC et les données, la vie privée fait référence au degré de confidentialité de vos informations (protection des données) et à l'étendue de leur partage (par exemple, publiquement ou uniquement par le responsable du traitement des données).
Stigmatisation	La stigmatisation, ou stigmate social, consiste à désapprouver ou à discriminer une personne ou un groupe de personnes sur la base de perceptions concernant cette personne ou le(s) groupe(s) auquel elle appartient.
Personnes vulnérables	Les personnes vulnérables sont celles qui, pour un certain nombre de raisons, courent un risque plus élevé de subir un préjudice que la majorité des personnes dans la société. Vous trouverez des exemples de groupes vulnérables plus loin dans ce guide (Tableau 3). Les personnes appartenant à certains groupes sociaux sont parfois qualifiées de "défavorisées" ou d'"exclues socialement".

Quelles sont les questions éthiques et juridiques liées aux TIC ?

Les TIC ont apporté de nombreux avantages dans nos vies. Elles ont permis de parler rapidement et à moindre coût à des personnes du monde entier ; elles nous ont donné un accès instantané à plus d'informations que nous n'aurions jamais pu imaginer ; elles ont permis des avancées considérables dans le domaine des soins de santé ; elles nous ont aidés à lutter contre la pauvreté et à apporter l'éducation à un nombre croissant de personnes dans le monde.

Pourtant, ces progrès n'ont pas été sans coûts. De nombreuses TIC ont besoin de données pour fonctionner et, par conséquent, les entreprises, les organisations, les chercheurs et les gouvernements sont de plus en plus nombreux à demander - ou simplement à prendre - nos données. Les données et les informations sont puissantes, et ceux qui les contrôlent sont de plus en plus capables de découvrir tous les aspects de notre vie, tant professionnelle que privée - et de tirer profit de ces informations, que ce soit financièrement, politiquement ou d'une autre manière.

Pour beaucoup de gens, les débats sur ces questions éthiques et juridiques sont difficiles à comprendre, ou sont considérés comme ennuyeux ou sans rapport avec leur vie quotidienne. En outre, les débats éthiques sur les TIC évoluent très rapidement, et il peut être difficile pour les gens de les

suivre. En conséquence, nous sommes souvent prompts à renoncer à nos droits en échange des nombreux avantages qu'apportent les TIC.

Mais à mesure que les TIC continuent de se répandre dans tous les aspects de notre vie, la demande croissante de nos données personnelles rend ces questions de plus en plus importantes. Qui s'empare de nos données ? Avec qui d'autre les partagent-ils ? Que font-ils tous avec ces données - et que puis-je faire pour les contrôler ?

Les TIC sont un domaine qui évolue rapidement et, à ce titre, les questions éthiques et juridiques qui les entourent sont elles aussi en constante évolution. Le tableau 2 présente quelques-unes des principales questions éthiques et juridiques qui se posent actuellement aux citoyens en matière de TIC.

Tableau 2. Questions éthiques et juridiques liées aux TIC

De nombreux citoyens n'ont qu'une compréhension limitée des questions liées aux TIC et/ou ne s'y intéressent pas.	Les questions relatives aux TIC sont souvent difficiles à comprendre pour les non-experts. Cela vaut tant pour les questions juridiques (par exemple, les détails des conditions d'utilisation en ligne) que pour les questions éthiques, comme la surveillance et le rôle futur de l'intelligence artificielle. Pour beaucoup, cela va de pair avec un manque d'intérêt pour ce qui peut être des sujets complexes ou des documents remplis de terminologie juridique tels que le RGPD. Dans d'autres cas, les citoyens peuvent vouloir en savoir plus, mais ne savent pas où trouver de l'aide pour comprendre ces questions. Cela a des répercussions, comme le fait de cliquer sur "J'accepte" sans avoir lu, ou sans avoir compris, les conditions générales ou la politique de confidentialité d'un site web. En outre, les gens peuvent ne pas connaître les lois en vigueur pour protéger leurs droits dans le monde numérique - ce qui rend plus difficile l'exercice de ces droits.
Il existe un certain nombre d'obstacles qui limitent la compréhension des citoyens	Pour de nombreuses personnes, il existe des obstacles majeurs qui les empêchent d'accéder à des informations supplémentaires sur les TIC et les droits numériques. La langue en est un : une grande partie de ces informations sont en anglais et dans d'autres grandes langues européennes, mais tout le monde en Europe ne maîtrise pas ces langues. En outre, la plupart de ces informations ne sont disponibles qu'en ligne. Pour les communautés hors ligne - celles qui ont un accès limité ou nul à internet - elles restent hors de portée. Ce manque d'accès aux informations accessibles via les TIC est un exemple de "fracture numérique".

Il existe un déséquilibre de pouvoir perçu entre les citoyens et les entreprises technologiques.	Les "géants de la technologie" - les grandes entreprises technologiques mondiales, telles que Facebook et Google - peuvent sembler très puissants. Pour certaines personnes, cela peut également être le cas pour des entreprises technologiques plus petites. Par conséquent, il peut être difficile de dire "non" ou "je ne suis pas d'accord" lorsque ces entreprises nous demandent des données. Les gens pensent qu'ils risquent de ne pas pouvoir utiliser leurs services, ou s'inquiètent du fait que ces entreprises auront de toute façon accès à leurs données. Ce sentiment d'impuissance est, bien entendu, accru lorsque les gens ne peuvent pas ou ne lisent pas les informations relatives à leurs droits numériques.
La diversité des citoyens signifie que les gens ont des préoccupations différentes en matière de TIC.	Les différents groupes de la société utilisent les TIC de manières très différentes - et ont donc des préoccupations, des problèmes et des défis différents en ce qui concerne l'utilisation des TIC. Fournir les informations dont chaque groupe ou individu a besoin, dans le format et la langue qu'il souhaite, est un défi. Par conséquent, une grande partie des informations sur les TIC et les droits numériques sont génériques, ce qui complique la tâche des personnes qui souhaitent trouver ce dont elles ont besoin.
Le paysage des TIC est en constante évolution	Les TIC et les droits numériques sont complexes. À cette complexité s'ajoute le fait que la technologie est en constante évolution et que nos données sont constamment utilisées de manière nouvelle et de plus en plus compliquée. Cela entraîne ses propres défis, notamment le fait qu'il y a toujours de nouvelles lois, procédures et évolutions que nous devons essayer de comprendre. Cette complexité est accrue en raison des différentes interprétations de ces droits, et des protections mises en place pour les garantir (par exemple, le RGPD) dans différents pays.

Source : Adapté du rapport de l'atelier COST Action/PANELFIT qui s'est tenu en mars 2020 ; complété par les autres ressources listées à la fin de ce guide.

Qui est vulnérable ?

Les défis éthiques et juridiques liés aux TIC concernent tout le monde, en Europe et au-delà. Pour les groupes vulnérables de la société, cependant, ces risques sont souvent encore plus aigus - et dans de nombreux cas, leur capacité d'adaptation à ces risques est plus faible. En outre, il est possible que certaines personnes vulnérables passent à côté des opportunités et des avantages que les TIC peuvent apporter si elles n'en sont pas conscientes, ou si leur crainte de ces risques l'emporte sur leur désir d'en bénéficier.

Mais qui est considéré comme vulnérable ? Il n'est pas simple de répondre à cette question car, pour un certain nombre de raisons, la vulnérabilité est complexe. L'encadré 1 présente un résumé de cette complexité, puis les facteurs qui y contribuent sont expliqués plus en détail.

Encadré 1. Comment "décortiquer" la vulnérabilité

Les points exposés ici ne couvrent pas tous les éléments de la vulnérabilité, mais soulignent qu'il s'agit d'un concept compliqué et aux multiples facettes. Le message général est que la vulnérabilité est un concept fluide et dynamique, et que la plupart des gens ne rentrent pas dans des catégories binaires et précises de vulnérabilité.

Nous suggérons plutôt de considérer la vulnérabilité comme un spectre : les individus ou les groupes peuvent avoir des niveaux élevés ou faibles de vulnérabilité, qui peuvent être fixes (statiques) ou changeants (dynamiques). La vulnérabilité est susceptible de changer au cours de la vie d'une personne : avec l'âge, en raison de l'évolution des circonstances personnelles, et en raison de facteurs indépendants de sa volonté.

Il convient également de noter que *chacun* est potentiellement vulnérable, et que son niveau de résilience - sa capacité à faire face à la vulnérabilité - est déterminé par son accès aux ressources (par exemple, les services publics disponibles dans un pays) et par des facteurs culturels (par exemple, ses réseaux de soutien).

Avant tout, il est important de se rappeler que tous les groupes et individus mentionnés dans ce guide sont avant tout des *personnes,* et que toute autre définition - en tant que personne concernée, personne vulnérable, voire citoyen - est secondaire.

Les causes de la vulnérabilité sont très variables

Les personnes peuvent être vulnérables de nombreuses façons différentes. Par exemple, la vulnérabilité peut être causée par des problèmes financiers (par exemple, le chômage, des dettes impossibles à gérer) ou des obstacles liés à la santé et aux capacités, comme la maladie, la vieillesse ou le handicap. D'autres causes de vulnérabilité peuvent être liées à l'emplacement, comme le fait de vivre dans des zones rurales éloignées avec peu d'équipements (par exemple, des hôpitaux, des écoles). Les causes de vulnérabilité peuvent être sociétales, comme les préjugés à l'égard des réfugiés, des étrangers ou des gens du voyage. Elles peuvent également être dues à une discrimination fondée (entre autres) sur la race, l'ethnicité, la nationalité, la classe, la caste, la religion, les croyances, le sexe, le genre, la langue, l'orientation sexuelle, l'identité de genre et les caractéristiques sexuelles.

Les personnes ou les groupes peuvent connaître plus d'une forme de vulnérabilité

La forme que prend la vulnérabilité d'une personne peut être complexe. Au niveau individuel, une personne peut être affectée par une mauvaise santé et une faible capacité financière. Ces vulnérabilités ont des impacts différents, mais sont souvent interconnectées ; en effet, une cause de vulnérabilité peut souvent en exacerber d'autres, créant ainsi un "cercle vicieux". Dans l'exemple cité, le manque d'argent peut entraîner une mauvaise santé (due, par exemple, à un régime alimentaire limité ou à des conditions de vie insalubres) et la mauvaise santé qui en résulte peut rendre plus difficile la recherche d'un emploi - ce qui, à son tour, augmente ou maintient la vulnérabilité financière de la personne.

La vulnérabilité peut varier au sein d'un groupe de la société

Les individus au sein d'un groupe vulnérable peuvent subir différents impacts, et niveaux d'impact, d'une situation commune. Par exemple, certains réfugiés en Europe peuvent être plus vulnérables que d'autres en raison d'une série de facteurs tels que : le pays dont ils sont originaires (par exemple, les raisons de leur départ et si cela a causé un traumatisme ou des problèmes psychologiques) ; le pays dans lequel ils vivent actuellement (par exemple, ses installations pour les réfugiés, l'attitude du public à l'égard des réfugiés) ; et leur éducation, leur formation et leurs compétences (par exemple, les compétences linguistiques, les qualifications professionnelles). Tous ces éléments influencent leur capacité à s'installer, à trouver du travail et à accéder aux services qui leur sont offerts. Ainsi, s'il est vrai de dire que "les réfugiés sont vulnérables", la gravité de cette vulnérabilité, et l'expérience qu'en ont les gens, varient considérablement au sein de ce vaste groupe. En effet, décrire un certain type de vulnérabilité à l'aide d'un terme général peut faire oublier les problèmes spécifiques des individus, ce qui rend la tâche plus difficile.

La vulnérabilité peut être dynamique

Si certaines vulnérabilités ne changent pas de manière significative au cours de la vie d'une personne (par exemple, les handicaps incurables), d'autres peuvent s'aggraver ou s'améliorer avec le temps. Par exemple, de nombreuses personnes voient leur situation personnelle changer, comme leur situation financière ou leur santé. Les facteurs externes qui affectent leur vulnérabilité peuvent également changer ; il peut s'agir du climat politique de leur pays, qui peut amener un gouvernement moins favorable aux groupes marginalisés. Dans d'autres cas, la cause d'une vulnérabilité peut devenir superflue avec le temps, comme un problème de santé qui s'améliore ou des chômeurs qui trouvent du travail, ce qui supprime ou réduit leur vulnérabilité financière.

Certains de ces changements sont prévisibles, comme l'augmentation de la vulnérabilité avec l'âge. Dans certains cas, cependant, la cause de la vulnérabilité peut être rapide et inattendue : les gens peuvent être frappés par des phénomènes indépendants de leur volonté, comme des événements climatiques extrêmes. Ces "chocs" peuvent créer une vulnérabilité à laquelle les gens ne se sont pas préparés.

La vulnérabilité peut être supposée

Lorsqu'on examine la vulnérabilité au sein d'une société, on est souvent tenté de supposer les caractéristiques de certains groupes - mais elles ne s'appliquent pas nécessairement à tous les membres de ce groupe. Par exemple, les réfugiés peuvent être bien éduqués et bien parler la langue de leur pays d'accueil. Cependant, ils sont susceptibles de partager d'autres caractéristiques vulnérables avec d'autres réfugiés, comme un accès plus limité aux ressources et aux opportunités d'emploi (par rapport aux non-réfugiés), ou des abus, de la négligence, de l'exploitation, des préjugés et de l'antagonisme de la part des autres membres de la société.

Certains groupes souvent considérés comme vulnérables doivent être soigneusement définis, et parfois même sous-catégorisés. Par exemple, les enfants et les jeunes (âgés de 16 à 25 ans) sont souvent identifiés comme vulnérables, mais la nature de la vulnérabilité variera considérablement selon qu'ils sont :

- des élèves des écoles, qui ne sont pas légalement capables de prendre toutes les décisions pour eux-mêmes.
- dans l'enseignement supérieur, ce qui peut entraîner du stress ou d'autres problèmes de santé mentale.
- des employés, souvent peu rémunérés ou précaires dans cette tranche d'âge.
- en dehors de l'éducation et de l'emploi, ce qui peut entraîner un certain nombre de vulnérabilités (financières, conditions de vie, problèmes de santé mentale, par exemple).

La vulnérabilité peut également être subjective et invisible. Une personne peut se sentir vulnérable, ou se classer comme telle, alors qu'une autre personne se trouvant dans une situation similaire (ou peut-être même pire) ne le sera pas. Dans le même temps, tout citoyen peut se considérer comme vulnérable, pour des raisons qui ne sont pas immédiatement évidentes pour les autres.

La vulnérabilité peut affecter la personne - mais aussi sa culture

Dans certains cas, ce ne sont pas (seulement) les individus d'un groupe qui sont vulnérables. Certains groupes peuvent trouver que leur patrimoine culturel est menacé, ou que l'accès à celui-ci l'est. Cela peut être dû à des menaces extérieures, comme le changement climatique : dans les régions polaires, c'est tout le mode de vie des populations autochtones qui est menacé. Les ressources culturelles des personnes peuvent également être vulnérables, comme leur langue, leurs structures et réseaux familiaux et sociaux, ainsi que leur patrimoine naturel et leur environnement.

Les groupes vulnérables en Europe

Tout en gardant cette complexité à l'esprit, il est souvent nécessaire d'identifier les groupes et les individus vulnérables. Alors, qui peut, ou devrait, être considéré comme "vulnérable" en Europe ? Il n'existe pas de définition unique de la vulnérabilité, mais une définition utile pour préparer le terrain est celle utilisée par l'UE[6] pour les migrants :

"Les mineurs, les mineurs non accompagnés, les personnes handicapées, les personnes âgées, les femmes enceintes, les parents isolés avec des enfants mineurs, les victimes de la traite des êtres humains, les personnes atteintes de maladies graves, les personnes souffrant de troubles mentaux et les personnes qui ont été soumises à la torture, au viol ou à d'autres formes graves de violence psychologique, physique ou sexuelle, comme les victimes de mutilations génitales féminines."

Sur la base de cette définition, le tableau 3 identifie plusieurs groupes vulnérables en Europe,[7] ainsi que les personnes qui connaissent certains types de vulnérabilité.[8] Ce tableau ne doit pas être considéré comme une liste complète des groupes vulnérables en Europe ; étant donné la nature changeante de la vulnérabilité, il serait impossible de la terminer. Toutefois, elle offre un point de départ utile pour réfléchir aux personnes qui sont vulnérables.

Le tableau 3 donne également un exemple de la manière dont leur vulnérabilité peut les affecter en termes de TIC (voir la section suivante pour plus de détails sur ce sujet). Les exemples donnés servent à illustrer les types possibles de vulnérabilité liée aux TIC pour chaque groupe ; de nombreux autres types sont susceptibles d'exister, en fonction du degré de vulnérabilité et des circonstances.

Nous n'avons pas tenté de classer ces groupes sous des rubriques ou des thèmes plus larges. Cela contredirait l'une de nos principales recommandations : la vulnérabilité doit être considérée comme dynamique et complexe, et non comme une "étiquette" à appliquer à certains groupes ou individus. Le fait de qualifier de grands groupes de la société de vulnérables peut, en fait, accroître la discrimination et la stigmatisation dont ils font l'objet.

Comment les questions éthiques et juridiques liées aux TIC affectent-elles les personnes vulnérables ?

Les questions éthiques et juridiques liées aux TIC - telles que celles relatives à la confidentialité des données, à leur commercialisation et à l'utilisation croissante de nouvelles technologies telles que la reconnaissance faciale - concernent tous les membres de la société. Mais, comme nous l'avons mentionné, les personnes et groupes vulnérables de la société sont souvent plus exposés que d'autres à des risques, et ce de différentes manières ; l'encadré 2 en présente quelques-unes.

Encadré 2. Comment les TIC affectent-elles les personnes vulnérables en particulier ?

- Ces personnes et ces groupes ne sont pas seulement vulnérables en eux-mêmes ; ils sont également plus vulnérables au fait que leurs données soient utilisées d'une manière qui les mette en danger (par exemple, une surveillance accrue). Bien qu'il s'agisse d'un risque pour tous les citoyens, les personnes vulnérables sont souvent confrontées à un risque plus élevé. Par exemple, elles peuvent être incapables de donner leur consentement, ou ne pas maîtriser la ou les langues nationales du pays dans lequel elles vivent.
- Les déséquilibres de pouvoir entre les personnes concernées et les responsables du traitement des données peuvent être exacerbés avec les personnes vulnérables. Par exemple, dans les cas où les données personnelles sont susceptibles d'être utilisées à mauvais escient par les responsables du traitement, les personnes vulnérables peuvent se trouver moins à même de contrôler ou d'empêcher cela, parce qu'elles ont moins de pouvoir, de connaissances ou de conscience de la question.
- Il existe un risque de (plus grande) stigmatisation, car les personnes sont placées dans des groupes à des fins de recherche et d'analyse.

Ces risques ne sont pas seulement liés à la nature de la vulnérabilité d'une personne, mais aussi au type de données la concernant qui sont collectées et utilisées. Certains types de données - comme les informations sur la religion, les antécédents médicaux ou l'orientation sexuelle d'une personne - peuvent présenter un risque plus important, en fonction du lieu et du contexte dans lesquels elles sont utilisées.

En outre, comme nous l'avons mentionné, la vulnérabilité peut changer au fil du temps, ce qui soulève des problèmes en termes de données personnelles. Des personnes ou des groupes qui ne sont pas vulnérables au moment où ils partagent leurs données peuvent le devenir par la suite. Par conséquent, les conditions dans lesquelles ils ont donné leur consentement à l'utilisation de leurs données peuvent ne plus s'appliquer. Les équipes de recherche qui manquent de ressources peuvent ne pas avoir le

temps, l'argent et, dans certains cas, les informations nécessaires pour mettre en œuvre des mesures garantissant le respect des données et des droits à la vie privée de leurs sujets.

Comme précédemment, le message est le suivant : la vulnérabilité est complexe ! Le tableau 3 met en évidence certaines des façons dont les groupes vulnérables de la société peuvent être particulièrement touchés par les questions éthiques et juridiques liées aux TIC et aux données. Nous ne disons pas qu'elles s'appliquent à tous les membres de ces groupes ; il s'agit simplement d'exemples qui mettent en évidence les façons dont la vulnérabilité, et la vulnérabilité liée aux TIC et aux données, peut se produire.

Tableau 3. Exemples de groupes vulnérables en Europe, et la nature de leurs vulnérabilités

Groupe vulnérable	Vulnérabilité possible	Vulnérabilité éventuelle en ce qui concerne les TIC et les données
Femmes	Les femmes enceintes ou allaitantes peuvent être, ou se sentir, plus vulnérables que les autres femmes, par exemple en raison de changements dans leur état de santé. Les femmes en âge de procréer sont plus exposées à la discrimination dans les processus d'embauche.	Les femmes qui ont subi une opération de changement de sexe peuvent avoir des données stockées à leur sujet qui ne reflètent plus leur statut.
Parents ou tuteurs célibataires / parents ou tuteurs d'enfants vulnérables ou de personnes à charge	Les tâches supplémentaires de soins peuvent leur laisser moins de temps et de ressources pour prendre soin d'eux-mêmes, ce qui accroît leur vulnérabilité.	Ils peuvent avoir moins de temps pour lire et comprendre les questions liées aux TIC.
Sans-abri	Les personnes dans cette situation sont souvent confrontées à des risques sanitaires plus importants, ainsi qu'à un risque accru de violence, de chômage et de pauvreté.	Il est probable qu'ils aient moins accès aux informations sur ces questions que les autres membres de la société. En outre, les données les concernant peuvent être collectées sans leur consentement éclairé (par exemple, lorsqu'elles utilisent les services pour sans-abri fournis par des organisations caritatives).
Personnes souffrant de dépendance(s), comme la toxicomanie et/ou l'alcoolisme	Les personnes vivant avec une dépendance sont confrontées à de nombreuses formes de vulnérabilité, telles que les risques sanitaires, un risque accru de violence, le chômage et la pauvreté.	Ils peuvent avoir une capacité réduite à comprendre les informations sur leurs droits en matière de TIC et de données.

Personnes souffrant ou risquant de souffrir de violences domestiques, d'abus psychologiques et/ou sexuels.	Les personnes confrontées à la violence et à l'abus sont susceptibles de connaître une série de vulnérabilités, telles que des problèmes de santé physique et mentale.	Dans certaines situations, l'accès des victimes à l'information peut être limité dans le cadre de l'abus qu'elles subissent ; par exemple, elles peuvent vivre avec un partenaire qui restreint ce qu'elles peuvent faire ou où elles peuvent aller.
Personnes qui ont été soumises à la torture, au viol ou à d'autres formes graves de violence psychologique, physique ou sexuelle, comme les victimes de mutilations génitales féminines	Parmi de nombreuses autres formes de vulnérabilité, les personnes qui en ont fait l'expérience sont susceptibles d'être confrontées à des traumatismes à long terme ou à d'autres dommages psychologiques, en plus des impacts sur leur santé physique.	Une réticence à partager leurs informations personnelles - par exemple, si elles sont migrantes ou n'ont pas de statut légal dans un pays - peut signifier que les victimes sont moins disposées à demander une aide médicale ou à informer la police de leur situation.
Victimes de la traite des êtres humains	L'absence de statut légal dans un pays peut signifier que ces personnes n'ont pas accès au soutien disponible ; par exemple, elles peuvent craindre d'être expulsées.	Ces personnes peuvent être incapables d'accéder aux services ou aux informations en ligne, en fonction des conditions dans lesquelles elles se trouvent (par exemple, détention illégale, esclavage moderne). En même temps, en n'étant pas "dans le système", elles peuvent être ignorées par les prestataires de services qui pourraient les aider.
Minorités religieuses	Il peut être difficile d'effacer les préjugés de la société à l'égard de ces groupes.	Certaines personnes peuvent considérer leur religion comme une affaire privée, mais certains processus de collecte de données inévitables exigent toujours que les personnes déclarent leur religion (par exemple, les réglementations fiscales en Allemagne).
Personnes LGBTQIA+[9] et minorités sexuelles	Les personnes appartenant à ce groupe sont toujours confrontées à une discrimination généralisée dans toute l'Europe.	Les nouvelles technologies qui violent la vie privée (par exemple, le profilage facial) peuvent être plus susceptibles de cibler ces groupes.

Populations transgenres	Les personnes appartenant à ce groupe sont toujours confrontées à une discrimination généralisée en Europe. Par exemple, la Hongrie a récemment adopté une loi mettant fin à la reconnaissance légale du statut de trans.[10]	Les cases à cocher homme/femme, que l'on trouve couramment sur de nombreux formulaires de collecte de données, sont discriminatoires à leur égard, tandis que le langage "traditionnel" utilisé dans de nombreuses situations en ligne (par exemple, il/elle, son/sa) fait de même.
Prisonniers	Les détenus sont coupés de leurs réseaux de soutien et sont souvent confrontés à des menaces supplémentaires, comme un risque accru de violence en prison.	Le fait d'être en prison peut réduire leur accès aux informations sur leurs données et leurs droits numériques.
Personnes sortant de prison	Les détenus nouvellement libérés peuvent manquer de réseaux de soutien et avoir du mal à trouver un emploi ou un logement.	Leur état de vulnérabilité peut réduire l'accès aux informations concernant leurs données et leurs droits numériques. En fonction de la durée de leur séjour en prison, elles peuvent ne pas être au courant des évolutions en matière de protection des données et de la vie privée.
Personnes peu ou pas éduquées.	Leur vulnérabilité est exacerbée par le fait qu'elles ne connaissent pas, ou ne sont pas en mesure de comprendre, les systèmes de soutien destinés à réduire leurs vulnérabilités. Elles ont généralement des revenus plus faibles, ce qui accroît leur vulnérabilité financière.	Les informations sur les TIC et les droits relatifs aux données ont tendance à être complexes et difficiles à comprendre ; un faible niveau d'éducation renforcera cette barrière.
Personnes qui sont en dehors de la formation et/ou de l'éducation	Cette situation peut exacerber de nombreux types de vulnérabilité, notamment sur le plan financier, de la santé (en particulier la santé mentale) et des réseaux de soutien.	Les informations sur les TIC et les droits numériques sont souvent transmises dans des cadres formels, tels que les écoles ou les collèges. Le fait d'être en dehors de ces structures réduit l'accès des personnes à ces informations.

Personnes mal informées, y compris celles qui ne sont pas en mesure de comprendre les informations fournies.	L'information, c'est le pouvoir ; ceux qui ne peuvent pas accéder aux informations destinées à les aider ou les comprendre sont, par conséquent, plus vulnérables que ceux qui le peuvent.	Cela vaut pour les informations numériques comme pour les formes d'information non numériques.
Personnes ayant des difficultés d'apprentissage, telles que la dyslexie, la dysorthographie, la dysgraphie et la dyscalculie.	Les difficultés d'apprentissage peuvent rendre les gens vulnérables de multiples façons. Par exemple, les personnes qui ne peuvent pas comprendre les informations destinées à les aider sont, par conséquent, plus vulnérables que celles qui le peuvent.	Ces difficultés d'apprentissage, ainsi que d'autres, font qu'il est plus difficile de trouver et/ou de comprendre les informations relatives aux droits des données, à la confidentialité des données, aux TIC, etc.
Groupes indigènes	Ces groupes menacés ou dont les effectifs diminuent peuvent avoir besoin d'une protection de leur patrimoine, par exemple dans des musées.	Les données de provenance - sur l'origine, la propriété et la garde des objets - ne sont pas toujours saisies par les TIC ; dans d'autres cas, les connaissances des populations autochtones peuvent être stockées à leur insu ou sans leur approbation.
Samis[11]	En tant que groupe minoritaire vivant dans l'une des régions les plus rudes d'Europe, les Samis connaissent de nombreuses formes de vulnérabilité. Un rapport du rapporteur spécial des Nations unies sur les droits des peuples autochtones a conclu que la Suède, la Norvège et la Finlande ne remplissent pas leurs objectifs déclarés de garantie des droits de l'Homme du peuple sami.[12]	Les Samis ont toujours été la cible de différents types de recherche. Il s'agit notamment de recherches basées sur les registres et les biobanques. Ces projets ont parfois contourné les considérations éthiques, par exemple en omettant d'indiquer clairement qu'ils visaient le peuple sami.
Minorités ethniques	Les minorités ethniques d'un pays sont souvent victimes de discrimination et peuvent présenter une prévalence plus élevée de plusieurs types de vulnérabilité (par exemple, faibles revenus, faible	Ils peuvent avoir un accès plus limité aux informations sur leurs droits en matière de données (par exemple, si elles ne sont pas disponibles dans leur première langue).

	niveau d'éducation, problèmes de santé, barrières linguistiques).	
Réfugiés	Les réfugiés sont souvent victimes de discrimination et peuvent présenter une prévalence plus élevée de plusieurs types de vulnérabilité (par exemple, faibles revenus, faible niveau d'éducation, problèmes de santé, barrières linguistiques).	Ils peuvent être réticents à fournir des données personnelles en raison de craintes quant à leur utilisation abusive. Cela peut les exclure des avantages potentiels que les TIC peuvent offrir.
Demandeurs d'asile	Les demandeurs d'asile peuvent connaître des problèmes de santé mentale ou des traumatismes, par exemple s'ils ont fui une zone de guerre ou une catastrophe.	Ils peuvent être réticents à fournir des données personnelles par crainte d'une utilisation abusive. Cela peut les exclure des avantages potentiels que les TIC peuvent offrir.
Migrants	La nature des vulnérabilités des migrants varie considérablement. Les migrants les plus pauvres peuvent connaître bon nombre des vulnérabilités auxquelles les réfugiés et les demandeurs d'asile sont confrontés, tandis que les migrants à revenu élevé peuvent connaître des vulnérabilités très différentes (par exemple, le stress, le ressentiment de la population locale).	Les barrières linguistiques peuvent accroître le risque d'utilisation abusive de leurs données personnelles. En outre, les réglementations relatives aux données et aux TIC dans leur nouveau pays peuvent être différentes de celles auxquelles ils sont habitués.
Membres des communautés de gens du voyage	Les communautés de gens du voyage sont souvent victimes de discrimination et peuvent se retrouver en dehors des systèmes de soutien officiels (par exemple, les écoles, les soins de santé).	Ils peuvent être réticents à fournir des données personnelles par crainte d'une utilisation abusive. Cela peut les exclure des avantages potentiels que les TIC peuvent offrir.
Membres de la communauté rom	Les Roms ont été historiquement persécutés dans toute l'Europe, ce qui rend de nombreux Roms plus vulnérables que d'autres populations, en termes de faibles revenus, d'emploi, de menaces pour leur bien-être et de nombreuses autres formes de vulnérabilité.	Ils peuvent être réticents à fournir des données personnelles par crainte d'une utilisation abusive. Cela peut les exclure des avantages potentiels que les TIC peuvent offrir.

Personnes malades ou blessées, y compris les patients hospitalisés et les patients de longue durée	Les problèmes de santé rendent les gens immédiatement vulnérables et peuvent exacerber d'autres types de vulnérabilité (par exemple, la perte de revenus).	Il se peut qu'elles ne soient pas en mesure de consentir à l'utilisation de leurs données, par exemple si elles sont sous sédatifs, confuses ou inconscientes. Ou bien, elles peuvent donner leur consentement trop facilement, par exemple si elles veulent que la recherche médicale les aide (vulnérabilité temporaire).
Personnes souffrant de maladies chroniques et/ou de longue durée, ou de maladies chroniques multiples	Les vulnérabilités sont déterminées par la nature et la gravité de l'affection. Par exemple, de nombreuses affections de ce type réduisent la capacité des personnes à travailler et à gagner un revenu.	Ces personnes sont souvent exclues des informations en ligne, selon que les outils TIC inclusifs sont mis en œuvre et disponibles ou non. Par exemple, les personnes épileptiques peuvent être vulnérables à l'exclusion de certaines ressources en ligne non inclusives en raison des flashs/lumières des écrans (épilepsie photosensible).[13]
Personnes vivant dans des établissements de soins	Les personnes vivant dans un établissement de soins résidentiels (également connu sous le nom d'établissement de vie assistée) se voient retirer de nombreuses décisions quotidiennes. Ce manque de contrôle sur leur vie peut accroître leur vulnérabilité à bien des égards (par exemple, leur alimentation, leurs soins de santé, leurs finances).	Pour de nombreuses personnes placées en institution, les données les concernant peuvent être contrôlées par d'autres personnes, comme les membres de la famille ou le personnel de leur maison de retraite. Cela réduit leur capacité à contrôler, voire à influencer, la manière dont leurs données personnelles sont utilisées.
Personnes souffrant de handicaps et de troubles, qu'ils soient physiques ou mentaux (ou les deux), et qu'ils soient temporaires ou permanents	Les vulnérabilités sont déterminées par la nature et la gravité des handicaps et des troubles. Par exemple, les personnes à mobilité réduite peuvent être dépendantes des autres, ce qui accroît leur vulnérabilité à l'exploitation ou à la négligence.	En raison de certains handicaps, les personnes peuvent avoir besoin d'aide pour accéder aux données ou les partager, ou pour comprendre les déclarations de confidentialité ou donner leur consentement. Cela réduit leur contrôle sur la confidentialité de leurs données.

Personnes dont la capacité de communication est limitée, par exemple en raison de troubles de la parole	Une capacité de communication limitée empêche les gens de demander des informations ou d'y contribuer dans toute une série de scénarios. Cela peut signifier que leurs besoins, leurs opinions ou leurs attentes ne sont pas pleinement pris en compte (par exemple, dans les débats publics).	Certaines limitations de la capacité de communication peuvent signifier que les personnes ont besoin d'aide pour accéder aux données ou les partager, ou pour comprendre les déclarations de confidentialité ou donner leur consentement. Cela réduit leur contrôle sur la confidentialité de leurs données.
Personnes malvoyantes ou aveugles	Si de nombreuses dispositions existent pour les personnes malvoyantes et aveugles, elles ne sont pas forcément disponibles ou abordables pour tous, ce qui accroît leur vulnérabilité.	Ils sont susceptibles d'utiliser un logiciel qui leur lit l'écran/la plate-forme, ce qui réduit la confidentialité de ces informations. En outre, ils peuvent voir leur accès à l'information limité, par exemple si les sites Web auxquels ils doivent accéder ne permettent pas au logiciel de tout lire (par exemple, les options dans les cases à cocher).
Personnes exclues par la langue ou confrontées à des barrières linguistiques	Les personnes qui ne parlent pas la langue de leur pays de résidence (par exemple, certains migrants et réfugiés, ou des minorités telles que les créolophones au Portugal) ont un accès réduit aux informations sur les mesures de soutien, ce qui accroît leur vulnérabilité.	Les locuteurs non natifs d'un pays, ou les locuteurs de langues minoritaires, manquent souvent d'informations dans leur propre langue sur leurs droits numériques.
Personnes qui ne maîtrisent pas l'anglais	L'anglais étant la langue prédominante en Europe, certaines informations peuvent n'être disponibles, ou être mises en évidence, que dans cette langue. Les personnes qui ne peuvent pas parler ou comprendre l'anglais peuvent se trouver désavantagées par rapport à celles qui le peuvent.	La plupart des informations sur les droits relatifs aux données et à la vie privée sont en anglais, ce qui désavantage ces groupes. Ils risquent également de constater qu'ils ont moins accès à la possibilité de partager leurs points de vue sur le développement et les progrès des TIC, si les enquêtes et les débats sont organisés en anglais.
Enfants / personnes à charge / mineurs	Les jeunes sont intrinsèquement vulnérables, car ils sont dépourvus de bon nombre des attributs qui réduisent la vulnérabilité (par exemple, la taille, la force, l'éducation achevée, l'indépendance, le revenu).	Les jeunes ne peuvent pas légalement consentir à l'utilisation de leurs données. Ils peuvent ne pas savoir comment se plaindre de l'utilisation abusive de leurs données, ou ne pas savoir qu'ils le peuvent.

Adultes émergents (18-25 ans)	Dans de nombreux pays, ce groupe d'âge a du mal à accéder aux avantages dont bénéficiaient les générations précédentes, tels que des emplois sûrs et bien rémunérés ou des logements abordables.	Le manque d'emploi et/ou de logement peut rendre plus difficile l'accès aux informations sur les droits numériques et les TIC (par exemple, en raison du manque d'accès à internet à la maison).
Adultes précoces (20-40 ans)	Dans de nombreux pays européens (par exemple, au Portugal et aux Pays-Bas), les personnes de ce groupe d'âge ont davantage tendance à être des travailleurs indépendants ou des freelances. En tant que tels, surtout dans les moments de crise (comme la pandémie de Covid-19), ils sont vulnérables aux changements dramatiques de leurs revenus. Elles peuvent également avoir de jeunes familles, et présentent donc un niveau de vulnérabilité accru (par exemple, sur le plan financier).	Inversement, ils peuvent potentiellement avoir des niveaux de compétences techniques et d'éducation plus élevés que les autres groupes d'âge. Cela signifie qu'ils sont moins susceptibles d'être vulnérables aux problèmes juridiques et éthiques liés à la confidentialité des données, aux TIC et à leurs droits numériques.
Personnes âgées, fragiles ou handicapées	La vieillesse est une étape de la vie intrinsèquement vulnérable, car les personnes peuvent devenir plus faibles et plus dépendantes des autres.	Si la vieillesse n'est pas toujours liée à l'analphabétisme numérique, il se peut que les personnes âgées soient moins sensibilisées aux questions juridiques et éthiques liées aux TIC, aux données et à la vie privée que la "génération numérique" qui a grandi avec cette technologie.
Personnes sans emploi ou sous-employées, à court et à long terme	Le chômage exacerbe d'autres formes de vulnérabilité, notamment la vulnérabilité financière et le logement. Il peut également entraîner des problèmes de santé et de santé mentale.	Les chômeurs peuvent ne pas bénéficier de la formation et de l'information sur les TIC dispensées sur leur lieu de travail. Ils peuvent ne pas avoir d'accès en ligne à la maison (pour des raisons financières), ce qui signifie qu'ils ne sont pas au courant des informations sur les TIC, qui sont de plus en plus partagées en ligne.
Personnes ayant un faible statut économique	Comme le chômage, un statut économique faible exacerbe d'autres formes de vulnérabilité, en particulier la vulnérabilité financière et le logement. Il peut également entraîner des problèmes de santé et	Les personnes de ce groupe peuvent ne pas avoir d'accès en ligne à la maison (pour des raisons financières), ce qui signifie qu'elles ne sont pas au courant des informations sur les TIC, qui sont de

	de santé mentale.	plus en plus partagées en ligne.
Clients et bénéficiaires de l'aide sociale	Les personnes prises en charge par l'aide sociale peuvent connaître de nombreuses autres formes de vulnérabilité (par exemple, une mauvaise santé, un faible revenu, un logement précaire).	Les personnes de ce groupe peuvent ne pas avoir accès à la formation et à l'information sur les TIC fournies par les lieux de travail, et/ou ne pas avoir d'accès en ligne à la maison (pour des raisons financières), ce qui signifie qu'elles ne sont pas au courant des informations sur les TIC, qui sont de plus en plus partagées en ligne.
Personnes analphabètes	Une grande partie des informations qui régissent nos vies et visent à nous soutenir sont fournies principalement sous forme écrite. L'analphabétisme est un obstacle majeur à l'accès à ces informations, ce qui rend ces personnes vulnérables. L'analphabétisme peut également être un facteur qui explique le statut économique inférieur de ces personnes.	Une grande partie des informations sur les questions juridiques et éthiques liées aux TIC est partagée sous forme écrite, notamment en ligne. L'illettrisme signifie que les gens seront moins conscients de ces informations et moins capables de les comprendre.
Personnes qui sont analphabètes en matière de numérique ou qui ont une expertise technologique limitée.	Une grande partie des informations qui régissent nos vies et visent à nous aider sont de plus en plus souvent fournies en ligne ; par exemple, les rendez-vous chez le médecin qui ne peuvent être pris qu'en ligne, ou les informations qui ne sont partagées que par le biais des réseaux sociaux.	Ces personnes risquent d'être laissées pour compte alors que les informations et les services se déplacent de plus en plus en ligne.
Communautés hors ligne	Il ne s'agit pas de la même vulnérabilité que l'illettrisme numérique : c'est une question d'accès/infrastructure, plutôt qu'une question de compétences/capacité. Toutefois, les communautés hors ligne seront confrontées à bon nombre des mêmes vulnérabilités que celles qui sont illettrées numériquement.	Ces personnes risquent d'être laissées pour compte alors que les informations et les services ont lieu de plus en plus en ligne.

Personnes ayant un accès limité aux infrastructures publiques	À titre d'exemple, les habitants des zones rurales de certains pays n'ont pas un bon accès aux infrastructures telles que les hôpitaux, les bibliothèques, le haut débit, la garde d'enfants et d'autres systèmes de soutien. Cela les rend relativement vulnérables, notamment lors de crises telles que la pandémie de Covid-19.	Le manque d'infrastructures peut s'étendre à un accès limité à internet (par exemple, haut débit faible ou coûteux) et à d'autres services TIC. Cela peut réduire l'accès des personnes aux informations sur leurs droits relatifs aux TIC, aux données et à la vie privée.
Communautés qui restent en dehors des processus de recherche	La science et la recherche servent de base à de nombreux éléments de la société, tels que les soins de santé, la gouvernance et l'éducation. En étant en dehors de ces processus, soit en tant que chercheurs, soit en tant que personnes concernées, ces communautés voient leur vie influencée par des processus de recherche dans lesquels elles n'ont ni intérêt ni voix au chapitre. En conséquence, les politiques fondées sur la recherche peuvent ne pas répondre à leurs besoins particuliers ou réduire leurs vulnérabilités spécifiques.	Cela est également vrai pour la recherche basée sur les TIC : les communautés qui n'ont pas d'intérêt ou de voix dans le processus, ou qui n'ont pas accès aux résultats, peuvent trouver que les impacts de cette recherche (par exemple, les politiques, les décisions de financement) ne répondent pas à leurs besoins ou ne les soutiennent pas. Par exemple, les enquêtes ou les questionnaires en ligne sont une méthode de recherche de plus en plus courante - mais excluent presque totalement les communautés hors ligne.
Personnes frappées par des phénomènes indépendants de leur volonté	Les événements ou phénomènes extrêmes peuvent entraîner une vulnérabilité inattendue. S'il peut s'agir de catastrophes naturelles (p. ex. volcans, pandémies mondiales) et de phénomènes climatiques extrêmes (p. ex. sécheresses, inondations), il peut également s'agir d'événements de la vie (p. ex. maladie inattendue, accidents, perte d'emploi, décès dans la famille). La nature inattendue de ces événements fait qu'il est difficile de s'y préparer, ce qui rend les gens moins résilients.	Au lendemain d'une crise, les gens peuvent être fatigués, stressés ou désorientés, et donc partager leurs données personnelles plus facilement (c'est-à-dire avec moins d'attention) ou le faire pour accéder à certains services (par exemple, l'aide post-catastrophe, les soins de santé d'urgence). Un exemple récent est la pandémie de Covid-19, au cours de laquelle les libertés individuelles et les questions de vie privée ont souvent été mises de côté pour lutter contre la propagation du virus.

Tout citoyen qui, pour quelque raison que ce soit, se considère comme vulnérable	La nature et la gravité de cette vulnérabilité, qu'elle soit liée aux TIC ou autre, dépendent de la perception du sujet. Toutefois, il est important de reconnaître que la vulnérabilité n'est pas une question simple et mesurable, mais qu'elle peut être subjective, cachée et personnelle.

Source : Adapté du rapport de l'atelier COST Action/PANELFIT qui s'est tenu en mars 2020 ; complété par les autres ressources listées à la fin de ce guide.

Que pouvez-vous faire ?

Il est clair que les personnes vulnérables devraient faire l'objet d'une plus grande attention dans les discussions éthiques et juridiques sur les TIC, et que des efforts plus importants devraient être déployés pour les inclure dans le développement et le déploiement des TIC et des nouvelles technologies qui les affecteront (par exemple, l'intelligence artificielle). Idéalement, il devrait y avoir des garanties spécifiques pour protéger les personnes vulnérables en termes de confidentialité des données et d'utilisation des données les concernant.

Toutefois, comme nous l'avons souligné, il est difficile - voire impossible - de créer une liste définitive de tous les groupes vulnérables de la société. Ce n'est même pas souhaitable, en raison de la nature dynamique de la vulnérabilité et du risque de simplifier à l'excès la complexité des situations des personnes, ou d'accroître le risque de stigmatisation. En tant que telles, les garanties spécifiques relatives aux droits numériques des personnes vulnérables pourraient mettre du temps à entrer en vigueur - si jamais elles le font.

En attendant, il existe des actions que tous les citoyens peuvent entreprendre pour veiller à ce que les droits numériques des personnes vulnérables soient respectés. La figure 1 présente une série d'actions.

Il existe également des mesures spécifiques que les responsables du traitement peuvent prendre pour protéger les personnes vulnérables. La figure 2 illustre certaines de ces mesures.

FIGURE 1	**FIGURE 2**
Personnes concernées	**Responsables du traitement des données**
Qui ? *Tous les citoyens, y compris les citoyens vulnérables et ceux qui ont la responsabilité de citoyens vulnérables.*	**Qui ?** *Chercheurs, employés, entreprises, autorités, organisateurs de projets, etc.*

Lorsque quelqu'un demande vos données, vérifiez les points suivants : Qui sont-ils ? Dans quel but vont-ils les utiliser ? Combien de temps vont-ils les conserver ? Avec qui vont-ils les partager ?	Au tout début du processus, posez la question suivante : "Qui sont les personnes concernées vulnérables dans mon projet, mon processus ou ma tâche ? En quoi sont-elles vulnérables ?
S'ils vous fournissent des informations générales (par exemple, les termes et conditions, les formulaires de consentement), vérifiez : Les comprenez-vous ? Sinon, demandez une version plus facile à comprendre (par exemple, dans votre langue maternelle).	Considérez les risques auxquels les membres de chaque groupe vulnérable seront confrontés lorsque vous utiliserez leurs données - et réfléchissez à la manière de les réduire ou de les surmonter.
Si vous n'êtes toujours pas sûr ou êtes mécontent de la manière dont vos données seront utilisées, renseignez-vous. Vous pouvez vous adresser à un bureau de conseil aux citoyens ou à votre autorité nationale de protection des données.	Lorsque vous demandez des données personnelles à des citoyens vulnérables, vérifiez : Ont-ils compris à quoi serviront leurs données ? Comment faire pour que ce soit plus simple à comprendre pour eux ? Ont-ils vraiment donné librement leur consentement à leur utilisation ?
Dans la plupart des cas, vous avez le droit de retirer votre consentement à l'utilisation de vos données. Avant de partager vos données, vérifiez : Comment puis-je retirer mon consentement par la suite ? Qui dois-je contacter ?	Ne cherchez pas de solutions concrètes et ne considérez pas le traitement de la vulnérabilité comme une "case à cocher" dans votre projet. Au contraire, considérez-la comme un processus continu qui doit être revu régulièrement.
Si vos droits en matière de données ont été violés immédiatement, contactez le bureau de protection des données correspondant. Si vous ne vous sentez pas à l'aise pour le faire, vous trouverez au tableau 4 une liste d'organisations susceptibles de vous aider.	Pensez à la protection des données pour les groupes vulnérables à chaque étape du projet : Cette activité présente-t-elle un risque pour les groupes vulnérables ? Comment puis-je y remédier ?

Ressources utiles

Il existe plusieurs organisations, sites web et projets destinés à aider les gens à comprendre leurs droits dans notre monde de plus en plus numérique, et qui soutiennent les groupes vulnérables de différentes manières. Nous avons inclus dans le tableau 4 une liste d'ONG que vous pouvez contacter et demander des informations/de l'aide en cas d'inconduite en matière de confidentialité des données. Si vous souhaitez en savoir plus sur ces sujets, nous vous recommandons les suivantes.

Tableau 4. Exemples d'organisations offrant un soutien aux groupes vulnérables en Europe.

Groupe vulnérable	ONG	Coordonnées de l'ONG (juste au cas où)
Femmes	Lobby européen des femmes : https://womenlobby.org/?lang=en	ewl@womenlobby.org
Parents ou tuteurs célibataires / parents ou tuteurs d'enfants vulnérables ou de personnes à charge	COFACE Familles Europe : https://coface-eu.org/about-us/	secretariat@coface-eu.org
Sans-abri	FEANTSA : https://www.feantsa.org/en/about-us/what-is-feantsa	information@feantsa.org
	Homeless in Europe International : https://www.homelessineurope.eu/	homelessineuropehope@gmail.com
Personnes souffrant de dépendance(s), comme la toxicomanie et/ou l'alcoolisme	Dianova International : https://www.dianova.org/	switzerland@dianova.org
Personnes souffrant ou risquant de souffrir de violences domestiques, d'abus psychologiques et/ou sexuels.	Femmes contre la violence en Europe : https://wave-network.org/	office@wave-network.org
	Rape Crisis Network Europe --> Ils ont également une longue liste d'organisations (certaines sont des ONG) : https://www.rcne.com/contact/countries/	Chaque organisation a sa propre adresse électronique
Personnes qui ont été soumises à la torture, au viol ou à d'autres formes graves de violence psychologique, physique ou sexuelle, comme les victimes de mutilations génitales féminines	Conseil international de réhabilitation pour les victimes de la torture : https://www.irct.org/	irct@irct.org
	Réseau européen End FGM : https://www.endfgm.eu/who-we-are/vision-and-mission/	https://www.endfgm.eu/resources/resource-items/contact/
Victimes de la traite des êtres humains	La Strada International : https://www.lastradainternational.org/	info@lastradainternational.org
Minorités religieuses	Minority Rights Group International : https://minorityrights.org/about-us/	minority.rights@minorityrights.org
Personnes LGBTQIA+[1] et minorités sexuelles	Vous avez ici une longue liste avec des ONG de différents pays : https://www.ilga-	

	europe.org/who-we-are/members.	
Populations transgenres	Transgender Europe : https://tgeu.org/	tgeu@tgeu.org
Prisonniers	Association européenne pour l'éducation en milieu carcéral : https://www.epea.org/epea/	secretary@epea.org
	Observatoire européen des prisons : http://www.prisonobservatory.org/	info@prisonobservatory.org
Personnes sortant de prison	Observatoire européen des prisons : http://www.prisonobservatory.org/	info@prisonobservatory.org
Personnes peu ou pas éduquées.	Waag - https://waag.org/en	https://waag.org/en/contact
Personnes qui sont en dehors de la formation et/ou de l'éducation	Waag - https://waag.org/en	https://waag.org/en/contact
Personnes mal informées, y compris celles qui ne sont pas en mesure de comprendre les informations fournies.	Association européenne pour l'intérêt des téléspectateurs (EAVI) : https://eavi.eu/about-us/	eavi@eavi.eu
Personnes ayant des difficultés d'apprentissage, telles que la dyslexie, la dysorthographie, la dysgraphie et la dyscalculie.	European Dislexia Association : https://eda-info.eu/about-the-eda/	eda-info@eda-info.eu
Groupes indigènes	Minority Rights Group International : https://minorityrights.org/about-us/	minority.rights@minorityrights.org
	Réseau européen des peuples indigènes : https://www.enip.eu/	enip@enip.eu
Sami[2]	Saami Coucil : https://www.saamicouncil.net/en/the-saami-council	saamicouncil@saamicouncil.net
Minorités ethniques	Minority Rights Group International : https://minorityrights.org/about-us/	minority.rights@minorityrights.org
	Réseau européen contre le racisme : enar-eu.org/About-us	info@enar-eu.org

Réfugiés	Conseil européen sur les réfugiés et les exilés : https://ecre.org/	vzahle@ecre.org
	RedCross Europe : https://redcross.eu/about	infoboard@redcross.eu
Demandeurs d'asile	Conseil européen sur les réfugiés et les exilés : https://ecre.org/	vzahle@ecre.org
	RedCross Europe : https://redcross.eu/about	infoboard@redcross.eu
Migrants	Plate-forme européenne des ONG sur l'asile et la migration : http://www.ngo-platform-asylum-migration.eu/	comms@migpolgroup.com
	RedCross Europe : https://redcross.eu/about	infoboard@redcross.eu
Membres des communautés de gens du voyage	Waag - https://waag.org/en	https://waag.org/en/contact
Membres de la communauté rom	Centre européen des droits des Roms : http://www.errc.org/	office@errc.org
Personnes malades ou blessées, y compris les patients hospitalisés et les patients de longue durée	Personnes cérébro-lésées et familles : https://bif-ec.com/about-2/	https://bif-ec.com/contact/
Personnes souffrant de maladies chroniques et/ou de longue durée, ou de maladies chroniques multiples	EUROFEA : https://www.euforea.eu/ngo	contact@euforea.eu
Personnes vivant dans des établissements de soins	AGE : https://www.age-platform.eu/about-age	info@age-platform.eu
Personnes souffrant de handicaps et de troubles, qu'ils soient physiques ou mentaux (ou les deux), et qu'ils soient temporaires ou permanents	Inclusion Europe : https://www.inclusion-europe.eu/what-we-do/	secretariat@inclusion-europe.org
Personnes dont la capacité de communication est limitée, par exemple en raison de troubles de la parole	Inclusion Europe : https://www.inclusion-europe.eu/what-we-do/	secretariat@inclusion-europe.org
Personnes malvoyantes ou aveugles	Union européenne des aveugles : https://www.euroblind.org/	ebu@euroblind.org
Personnes exclues par la langue ou confrontées à des barrières linguistiques	Conseil européen sur les réfugiés et les exilés : https://ecre.org/	vzahle@ecre.org

Personnes qui ne maîtrisent pas l'anglais	Conseil européen sur les réfugiés et les exilés : https://ecre.org/	vzahle@ecre.org
Enfants / personnes à charge / mineurs	Eurochild : https://www.eurochild.org/	info@eurochild.org
Adultes émergents (18-25 ans)	ERYICA - Agence européenne pour l'information et le conseil des jeunes : https://www.eryica.org/eryica	secretariat@eryica.org
Adultes précoces (20-40 ans)	ERYICA - Agence européenne pour l'information et le conseil des jeunes : https://www.eryica.org/eryica	secretariat@eryica.org
Personnes âgées, fragiles ou handicapées	AGE : https://www.age-platform.eu/about-age	info@age-platform.eu
Personnes sans emploi ou sous-employées, à court et à long terme	Le Réseau européen de lutte contre la pauvreté (EAPN) : https://www.eapn.eu/who-we-are/what-is-eapn/	https://www.eapn.eu/who-we-are/contact-us/
Personnes ayant un faible statut économique	Le Réseau européen de lutte contre la pauvreté (EAPN) : https://www.eapn.eu/who-we-are/what-is-eapn/	https://www.eapn.eu/who-we-are/contact-us/
Clients et bénéficiaires de l'aide sociale	Services sociaux européens : https://www.socialserviceseurope.eu/why-we-do-it	info@socialserviceseurope.eu
Personnes analphabètes	World Literacy Foundation (Cette ONG est mondiale, pas européenne, mais elle a un bureau au Royaume-Uni) : https://worldliteracyfoundation.org/about-us/	Formulaire de contact en fin de page : https://worldliteracyfoundation.org/about-us/
Personnes qui sont analphabètes en matière de numérique ou qui ont une expertise technologique limitée.	Tout numérique : https://all-digital.org/about-us/	contact@all-digital.org
	Réseau européen d'apprentissage numérique : http://dlearn.eu/	http://dlearn.eu/contact/
Communautés hors ligne	Bureau européen de la CROIX-ROUGE	+32 (0) 2 230 54 64
Personnes ayant un accès limité aux infrastructures publiques	PREPARE - Partenariat pour l'Europe rurale : http://www.preparenetwork.org/partnership/partners#ecovast	Kim.Smedslund@suomenkylat.fi
	Conseil européen pour le village et la petite ville : http://www.ecovast.org/english/	valeriecarter@ecovast.org

	about_e.html	
Communautés qui restent en dehors des processus de recherche	Centre européen pour les questions relatives aux minorités : https://www.ecmi.de/	info@ecmi.de
Personnes frappées par des phénomènes indépendants de leur volonté	Réseau Action Climat (RAC) Europe : https://caneurope.org/about-us/	info@caneurope.org
Tout citoyen qui, pour quelque raison que ce soit, se considère comme vulnérable	Waag - https://waag.org/en	https://waag.org/en/contact

Personnes et groupes vulnérables

Statewatch encourage la publication d'articles d'investigation et de recherche critique en Europe dans les domaines de l'État, de la justice et des affaires intérieures, des libertés civiles, de la responsabilité et de l'ouverture. Disponible en anglais.www.statewatch.org/about/

Le site web "**Protection sociale et droits de l'Homme"** contient un guide sur les groupes défavorisés et vulnérables de la société. Disponible en anglais.

https://socialprotection-humanrights.org/key-issues/disadvantaged-and-vulnerable-groups/

Ces vidéos de l'initiative pour l'accessibilité du web explorent les effets d'une plus grande accessibilité du web et les avantages pour tous, à l'aide d'exemples tirés de diverses situations. Disponible en anglais.

www.w3.org/WAI/perspective-videos/

Questions juridiques et éthiques concernant les TIC, les données et la vie privée

Le projet **Global Data Justice** se concentre sur les divers débats et processus qui se déroulent autour de la gouvernance des données dans différentes régions, en dégageant les principes et besoins primordiaux qui peuvent pousser la gouvernance des technologies de données dans le sens de la justice sociale. Disponible en anglais. https://globaldatajustice.org/

Le **Data Justice Lab** examine la relation entre la "datafication" et la justice sociale, ainsi que les politiques et les impacts des processus basés sur les données et du Big Data. Leur site web contient de nombreuses publications utiles, ainsi que des informations sur les événements à venir. Disponible en anglais. https://datajusticelab.org/

Le service d'assistance téléphonique sur la sécurité numérique d'Access Now travaille avec des particuliers et des organisations du monde entier pour assurer leur sécurité en ligne. Si vous êtes en

danger, elle peut vous aider à améliorer vos pratiques de sécurité numérique. Si vous êtes déjà attaqué, elle fournit une assistance d'urgence à réponse rapide. Disponible en arabe, anglais, français, allemand, italien, portugais, russe, espagnol, tagalog. www.accessnow.org/help/

Le kit de désintoxication des données de Tactical Tech propose des mesures quotidiennes que vous pouvez prendre pour contrôler votre vie privée numérique, votre sécurité et votre bien-être d'une manière qui vous convient. Disponible en 35 langues. https://datadetoxkit.org/en/home

Le **Future of Privacy Forum** et la **FPF Education and Innovation Foundation** sont des catalyseurs du leadership et de la recherche dans le domaine de la protection de la vie privée, et font progresser les pratiques de données fondées sur des principes à l'appui des technologies émergentes. Disponible en anglais. https://fpf.org/resources/

Le réseau **European Digital Rights** (EDRi) défend les droits fondamentaux à l'ère numérique, plaide en faveur de lois et de politiques appropriées et sensibilise aux principales questions ayant un impact sur les droits numériques. Disponible en anglais. https://edri.org/

Le guide de protection des données de **Privacy International** contient une multitude d'informations utiles sur les questions relatives à la protection des données. Disponible en anglais.

https://privacyinternational.org/report/2255/data-protection-guide-complete

Autres lectures

Si vous souhaitez en savoir plus sur certaines des questions soulevées dans ce guide, les contributeurs de celui-ci vous suggèrent les articles suivants comme bon point de départ.

Cet article de **Privacy International** examine comment les politiques d'immigration basées sur les données conduisent régulièrement à un traitement discriminatoire des migrants, en mettant l'accent sur le Royaume-Uni. https://privacyinternational.org/long-read/4000/10-threats-migrants-and-refugees

Cet article publié sur le site de l'**Alliance Data-Pop** est le résumé d'un chapitre de livre intitulé "Group privacy in the age of Big Data". Il traite de la manière dont le Big Data brouille les frontières entre les données individuelles et les données collectives, et de ce qui peut être fait à ce sujet.

https://datapopalliance.org/item/group-privacy-in-the-age-of-big-data/

Cet article du **Réseau européen de journalisme de données**, intitulé "The uncountable : How Covid-19 affected migrants and refugees' health" fournit un exemple de la façon dont les vulnérabilités s'exacerbent souvent les unes les autres. Disponible en anglais, français, allemand et italien.

www.europeandatajournalism.eu/eng/News/Data-news/The-uncountable-How-Covid-19-affected-migrants-and-refugees-health

Continuer à regarder et à écouter

Les chats mensuels PANELFIT ont couvert un large éventail de sujets autour des données, des TIC, de la vie privée et des droits. L'ensemble de la série peut être revu - ou, si vous préférez, écouté - via le site web PANELFIT. Disponible en anglais.

www.panelfit.eu/2020/03/23/monthly-chats/

Remerciements

Sources d'information utilisées pour ce guide

Le projet PANELFIT a rassemblé les informations contenues dans ce guide à partir des sources suivantes (les sources spécifiques sont indiquées dans le texte).

Conférences et ateliers

- Un atelier PANELFIT sur la "Création d'un dossier d'information des citoyens sur les questions éthiques et juridiques autour des TIC : que faut-il inclure ?", les 9 et 10 mars 2020 à Berlin, en Allemagne.
- Une intervention sur les populations vulnérables par le Dr Jedrzej Niklas, Département des médias et des communications, LSE, Royaume-Uni (anciennement Université de Leeds), lors d'un atelier PANELFIT, le 5 juin 2019, à Bilbao, Espagne.
- Communication personnelle avec le professeur Anna Lydia Svalastog, Département de la santé et des études sociales, Collège universitaire d'Østfold, Norvège.
- Communication personnelle avec le professeur Iñigo de Miguel Beriain, département de droit public Université du Pays basque, Espagne.
- Révision de la version finale et commentaires constructifs : Professeur Gianclaudio Malgieri, EDHEC Business school ; Aurelie Pols, membre du conseil d'administration du Center for Privacy &Cybersecurity ; Dr. Anna Berti Suman, The European Comission JRC et Marko Šijan AZOP.

Documents

- Berti Suman, A et Pierce, R (2018) "Challenges for citizen science and the EU Open Science Agenda under the GDPR", *European Data Protection Law Review* 4(3) : 284-95, https://doi.org/10.21552/edpl/2018/3/7 (accès libre).
- Malgieri, G et Niklas, J (2020) "Vulnerable data subjects", *Computer Law & Security Review* 37 : 105415, https://doi.org/10.1016/j.clsr.2020.105415 (accès libre).
- Milan, S et Terré, T (2017) "Big Data from the South : Le début d'une conversation que nous devons avoir", DataActive, 16 octobre, https://data-activism.net/2017/10/bigdatasur/ (accès libre).
- Peroni, L et Timmer, A (2013) "Vulnerable groups : The promise of an emerging concept in European Human Rights Convention law", *International Journal of Constitutional Law* 11(4) : 1056-85, https://doi.org/10.1093/icon/mot042 (accès libre).
- Consortium PANELFIT (2020) "D5.2 Analyse critique du cadre réglementaire de la protection des données dans le domaine des TIC (version consolidée)", Bilbao, Espagne.

Vidéos et podcasts

- Podcast PANELFIT avec Gianclaudio Malgieri, "Les personnes concernées vulnérables et le droit européen", 27 février 2020. Disponible à l'adresse suivante : www.youtube.com/watch?v=fqLfvF-cS70&feature=emb_title

Photos

Page 1 : © pixabay.com ; geralt-9301 / stocksnap-894430 / geralt-9301 / geralt-9301/ josemdelaa-2004715/ vipragen-13256880/

Contributeurs

Nous tenons à remercier les personnes suivantes pour leur aide à la rédaction de ce guide :

Alexandra Castañeda, Andreas Matheus, Andrzej Klimczuk, Anna Berti Suman, Annelies Duerinckx, Carolina Doran, Christoforos Pavlakis, Corelia Baibarac-Duignan, Elisabetta Broglio, Federico Caruso, Gefion Thuermer, Helen Feord, Janice Asine, Jaume Peira, Karen Soacha, Katerina Zourou, Katherin Wagenknecht, Katrin Vohland, Linda Freyburg, Marcel Leppée, Marta Camara Oliveira, Mieke Sterken, Tim Woods

Avis de non-responsabilité

Ce projet a été financé par le programme de recherche et d'innovation Horizon 2020 de l'Union européenne dans le cadre de la convention de subvention n° 788039. Ce document ne reflète que le point de vue de l'auteur et l'Agence n'est pas responsable de l'usage qui pourrait être fait des informations qu'il contient.

L'atelier qui s'est tenu à Berlin, en mars 2020, a été organisé grâce à une collaboration entre : l'European Citizen Science Association (ECSA), l'action COST 15212, l'Institut des sciences de la mer (ICM-CSIC), et les projets PANELFIT et EU-Citizen.Science. Le soutien financier a été fourni par PANELFIT (accord de subvention de l'UE 788039) et l'action COST 15212 (soutenue par la coopération européenne en science et technologie).

Consortium PANELFIT (2021)
Cette œuvre est soumise à une licence CC BY 4.0 : https://creativecommons.org/licenses/by/4.0/

Dossiers thématiques

1. Commercialisation des données : opérateurs téléphoniques et données personnelles

Que deviennent les données collectées via nos portables ?

Abstract: Certaines entreprises de téléphonie ont eu recours, par le passé, à des pratiques peu scrupuleuses à l'égard des données à caractère personnel de leurs clients. Même si la situation s'est améliorée sur ce plan en Europe, il est toujours important de savoir à quoi nous nous engageons lorsque nous signons un nouveau contrat.

Link: https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/How-phone-companies-use-our-personal-data

Author: Gianluca De Feo, Federico Caruso (OBCT(CCI)

Text:

À quelques exceptions près, le smartphone fait l'objet d'une utilisation assez intensive et continue par chacun d'entre nous. Cet appareil est en mesure de recueillir des données aussi nombreuses que variées à notre sujet, qui peuvent ensuite être vendues et utilisées de différentes façons pour créer une valeur ajoutée.

Les données récoltées sont très diverses : données de position, de navigation, biométriques, comportementales, etc. Il est ensuite possible d'en tirer des informations très sensibles (orientation sexuelle, idées politiques, appartenance à des minorités ou à des groupes vulnérables, état de santé...) qui peuvent servir à envoyer des messages ciblés aux utilisateurs. L'exemple le plus marquant à cet égard est celui de Cambridge Analytica, une agence anglaise qui, en 2016, a reçu de Facebook les données à caractère personnel de plus de 50 millions d'utilisateurs. Ces données ont ensuite été utilisées pour tenter d'influencer les votes qui ont conduit à l'élection de Donald Trump à la présidence des États-Unis.

Au cours des dernières années, des progrès ont été réalisés en matière de confidentialité des données des utilisateurs. Cette évolution est due aussi bien aux nouveautés introduites par l'Union européenne - notamment l'entrée en vigueur en 2018 du règlement général sur la protection des données (RGPD)

– qu'à l'initiative de grandes entreprises technologiques, comme Apple. Cette dernière, par exemple, a décidé en 2019 de rendre plus complexe la géolocalisation des utilisateurs à travers les applis de son « App Store ». Mais s'il est vrai que la confidentialité des données est protégée par ce biais, on ne peut s'empêcher d'y voir également une manœuvre pour écarter les entreprises concurrentes qui fournissent des services similaires aux siens.

Dans quel but les opérateurs collectent-ils nos données ?

Comme auparavant pour les téléphones classiques, un abonnement doit être souscrit auprès d'un opérateur pour pouvoir utiliser un smartphone. Chaque pays possède ses propres fournisseurs, filiales de groupes industriels plus ou moins importants, ayant chacun sa propre politique en matière de traitement des données à caractère personnel.

Le traitement des données est un sujet particulièrement sensible pour les opérateurs de téléphonie. Ceux-ci ont en effet la possibilité d'utiliser ces données à des fins de profilage pour proposer des services « sur mesure » ou envoyer des messages publicitaires ciblés. Mais ils peuvent tout aussi bien les céder ou les vendre à d'autres sociétés qui, à leur tour, les exploitent pour leur apporter une valeur supplémentaire. Ainsi ces dernières peuvent, par exemple, fournir des listes de noms à des centres d'appel qui communiqueront ensuite aux utilisateurs des messages commerciaux souvent jugées indésirables.

Des pratiques licites, illicites ou problématiques

Ces dernières années, des scandales liés à des pratiques peu scrupuleuses ont prouvé combien le marché des données était juteux pour les entreprises de téléphonie (comme pour d'autres types d'entreprises). La société espagnole Telefónica, notamment, avait lancé sur le marché allemand une appli qui récompensait les utilisateurs consentant à partager leurs données personnelles.

L'entrée en vigueur du RGPD en Europe a eu un effet dissuasif sur de telles pratiques, désormais passibles d'amendes de la part des autorités nationales chargées de la protection de la vie privée. Malgré tout, des cas problématiques se présentent encore régulièrement dans tous les secteurs. Toujours dans le domaine de la téléphonie, une enquête de Netzpolitik de 2021 a révélé qu'en Allemagne, la société O2 avait tendance à présenter à ses clients une série de cases « pré-cochées » destinées à assurer leur consentement à toutes les utilisations possibles de leurs données à caractère personnel.

Dans un autre ordre d'idée, la pandémie a mis en exergue l'importance des données personnelles. Durant cette période, les compagnies de téléphonie ont communiqué aux autorités des données

agrégées sur la mobilité des personnes sans donner trop d'explications sur leurs finalités ni leur durée de conservation. Il s'agissait évidemment de données anonymisées, mais plusieurs études récentes semblent donner raison aux experts qui s'inquiètent de la possibilité de réidentifier les personnes, y compris dans ces grands ensembles de données. Même si cette crainte ne se traduisait pas dans les faits, cette simple faculté constituerait une réelle menace, surtout dans un contexte marqué par une augmentation des attaques informatiques.

Que contiennent les politiques de confidentialité des opérateurs italiens ?

Il faut se rendre à l'évidence : peu d'entre nous lisent et comprennent réellement toutes les dispositions et clauses de consentement qui accompagnent notre signature au moment d'acheter une carte SIM ou de changer d'opérateur. D'où notre souhait d'analyser les politiques de confidentialité des entreprises de télécommunication portant sur les services de téléphonie et les applications (dont l'installation est recommandée par la quasi-totalité d'entre elles à des fins de gestion du profil). Nous évaluerons ainsi la quantité et le type de données collectées, ainsi que le caractère exhaustif des informations.

Nous nous sommes concentrés sur les quatre principaux opérateurs de téléphonie mobile : Orange, Bouygues télécom, SFR et Free Mobile, qui représentent à eux seuls plus de 90 % du marché français. Dans la plupart des cas, les opérateurs appliquent les mêmes conditions, pour le meilleur et pour le pire. Ainsi, si celles-ci sont énoncées assez clairement pour ce qui est du traitement des données de localisation, de profilage, de navigation ou pour ce qui est du retrait du consentement, de l'accès aux données personnelles et des réclamations. En revanche, les politiques concernant les données biométriques et comportementales, ainsi que – pour ce qui est de Free Mobile et de SFR – pour l'échange de données avec d'autres sociétés du groupe sont absentes ou peu claires.

Comment les compagnies de téléphone françaises collectent et utilisent les données personnelles, selon leur politique de confidentialité

Cliquez sur les cartes pour obtenir plus d'informations et lire des extraits des politiques de confidentialité.

Légende:
🔴 données collectées, transférées ou informations non communiquées
⚫ non spécifié ou pas clair

Orange	Bouygues	SFR	Free Mobile
Orange S.A.	Bouygues Group	Altice	Iliad S.A.
🔴 Données de localisation	🔴 Données de localisation	🔴 Données de localisation	🔴 Données de localisation
⚫ Données biométriques	⚫ Données biométriques	⚫ Données biométriques	⚫ Données biométriques
🔴 Données à des fins de profilage	🔴 Données à des fins de profilage	🔴 Données à des fins de profilage	🔴 Données à des fins de profilage
🔴 Données de navigation Internet	🔴 Données de navigation Internet	🔴 Données de navigation Internet	🔴 Données de navigation Internet
⚫ Données comportementales	⚫ Données comportementales	⚫ Données comportementales	⚫ Données comportementales
🔴 Vente ou transfert de données personnelles à des tiers	🔴 Vente ou transfert de données personnelles à des tiers	🔴 Vente ou transfert de données personnelles à des tiers	🔴 Vente ou transfert de données personnelles à des tiers
🔴 Échange de données avec d'autres sociétés du groupe	🔴 Échange des données avec d'autres sociétés du groupe	⚫ Échange des données avec d'autres sociétés du groupe	⚫ Échange des données avec d'autres sociétés du groupe
🔴 Informations sur le retrait du consentement	🔴 Informations sur le retrait du consentement	🔴 Informations sur le retrait du consentement	🔴 Informations sur le retrait du consentement
🔴 Informations sur les modalités d'accès aux données personnelles	🔴 Informations sur les modalités d'accès aux données personnelles	🔴 Informations sur les modalités d'accès aux données personnelles	🔴 Informations sur les modalités d'accès aux données personnelles
🔴 Informations sur la manière de déposer une réclamation	🔴 Informations sur la manière de déposer une réclamation	🔴 Informations sur la manière de déposer une réclamation	🔴 Informations sur la manière de déposer une réclamation

Source: EDJNet elaboration

EUROPEAN DATA JOURNALISM NETWORK
EUROPE EXPLAINED THROUGH DATA

Les problèmes se posent réellement au moment de la souscription d'un abonnement ou de l'achat d'une carte prépayée, lorsque l'utilisateur est invité à cocher une case qui autorise le traitement de ses données à caractère personnel à des fins commerciales, par exemple. En la cochant, il autorise l'opérateur à exploiter non seulement ses données personnelles, mais aussi celles de navigation et de position, qui permettent de connaître ses habitudes ou préférences d'achat. C'est par ce biais que des annonces publicitaires ciblées pourront lui être soumises par la suite. Ses données pourront de surcroît être cédées à des tiers (souvent difficiles à identifier ou présentés de manière générique) qui, à leur tour, pourront les utiliser à des fins commerciales, parfois même plusieurs années après la fin du contrat.

Les politiques de confidentialité sur les applications des opérateurs italiens

Les sociétés de téléphonie invitent souvent leurs clients à télécharger des applications pour leur smartphone, nécessaires en vue de surveiller leur consommation de données mobiles, connaître l'état

des bonus activés, etc. Ces applis disposent de leur propre politique de confidentialité. Celle-ci peut être différente, semblable ou identique à celle qui s'applique aux services proprement dits. Après les avoir également analysées, nous avons présenté les résultats dans le graphique ci-dessous, en ajoutant une catégorie spécifique aux smartphones : les pisteurs. Ces derniers sont des logiciels qui collectent des données sur l'utilisateur de l'application (vous trouverez des explications plus détaillées sous ce lien). Il en existe de différents types. Certains recueillent des données à des fins d'identification de l'utilisateur, créent un profil pour lui présenter de la publicité ciblée et permettent de déterminer la position géographique d'un mobile : ceux-là sont les plus controversés et nous les avons donc placés au cœur de notre analyse.

Nous avons pu examiner les applications et relever le nombre et le type de pisteurs qu'elles contiennent grâce à un outil conçu par εxodus. Orange et Bouygues télécom mènent le classement pour ce qui est du nombre de pisteurs : quatre chacun, dont trois consacrés à l'analyse et un à la publicité (Bouygues). SFR suit avec trois pisteurs et Free mobile avec deux, dont un consacré à la publicité. Seul Orange dispose d'un pisteur de localisation, lié à une marque de téléphone (Huawei).

Comment les applications des compagnies de téléphone françaises collectent et utilisent les données personnelles, selon leur politique de confidentialité

Tapez sur les cases pour obtenir plus d'infos et lire des extraits des politiques de confidentialité

Légende :
🔴 données collectées, transférées ou informations non données
🟡 données collectées ou transférées avec le consentement de l'utilisateur ou juste à certaines fins spécifiques, données cryptées ou informations partielles données
⚫ non spécifié ou pas clair.

Orange	Bouygues Telecom	SFR	Free Mobile
🔴 Données de localisation	🔴 Données de localisation	🔴 Données de localisation	🔴 Données de localisation
🟡 Données biométriques	⚫ Données biométriques	⚫ Données biométriques	🔴 Données biométriques
🔴 Données à des fins de profilage	🔴 Données à des fins de profilage	🔴 Données à des fins de profilage	🔴 Données à des fins de profilage
🔴 Données de navigation Internet	🔴 Données de navigation Internet	🔴 Données de navigation Internet	🔴 Données de navigation Internet
⚫ Données comportementales	⚫ Données comportementales	⚫ Données comportementales	⚫ Données comportementales
🔴 Vente ou transfert de données personnelles à des tiers	🔴 Vente ou transfert de données personnelles à des tiers	🔴 Vente ou transfert de données personnelles à des tiers	🔴 Vente ou transfert de données personnelles à des tiers
⚫ Échange de données avec d'autres sociétés du groupe	⚫ Échange de données avec d'autres sociétés du groupe	🔴 Échange de données avec d'autres sociétés du groupe	🔴 Échange de données avec d'autres sociétés du groupe
🔴 Informations sur le retrait du consentement	🔴 Informations sur le retrait du consentement	🔴 Informations sur le retrait du consentement	🔴 Informations sur le retrait du consentement
🔴 Informations sur les modalités d'accès aux données personnelles	🔴 Informations sur les modalités d'accès aux données personnelles	🔴 Informations sur les modalités d'accès aux données personnelles	🔴 Informations sur les modalités d'accès aux données personnelles
🔴 Informations sur la manière de déposer une réclamation	🔴 Informations sur la manière de déposer une réclamation	🔴 Informations sur la manière de déposer une réclamation	🔴 Informations sur la manière de déposer une réclamation
6	5	4	2

Source: EDJNet elaboration • Iliad doesn't have a mobile phone app

EUROPEAN DATA JOURNALISM NETWORK
EUROPE EXPLAINED THROUGH DATA

Les sanctions à l'encontre des pratiques illicites

À ce jour, les autorités nationales des États membres de l'UE ont infligé plusieurs amendes d'un montant considérable à des compagnies de téléphonie qui avaient enfreint les dispositions du RGPD.

En 2020, le contrôleur italien de la protection des données à caractère personnel a condamné Tim à une amende de près de 28 millions d'euros après avoir reçu de nombreuses plaintes d'utilisateurs mécontents de démarchages téléphoniques indésirables, en violation des règles en matière de gestion des données. Une amende de 4,5 millions d'euros a été infligée à Fastweb pour des motifs similaires en 2021. En 2020, l'autorité polonaise a adressé une amende de 443 000 euros à la société Virgin Mobile parce qu'elle n'avait pas garanti la sécurité des données personnelles de ses abonnés. Fin 2021, en France, la Commission nationale de l'informatique et des libertés a prononcé à l'encontre de Free Mobile une amende de 300 000 euros après avoir constaté un manquement au droit d'accès et au droit d'opposition au traitement des données. Les amendes les plus récentes, enfin, ont été infligées à la société grecque Ote et à sa filiale Cosmote (6 millions et 3,25 millions d'euros, respectivement) en raison d'un certain nombre d'irrégularités survenues à la suite d'une attaque informatique ayant causé la perte de 30 gigaoctets de données personnelles.

Méthodologie

Nous avons sélectionné les quatre principaux opérateurs de téléphonie mobile français (opérateurs historiques, possédant également l'infrastucture mobile : Orange, SFR, Bouygues télécom et Free mobile). Nous avons analysé les politiques de confidentialité relatives aux services de téléphonie mobile qui figurent sur le site de chaque opérateur. Nous avons aussi examiné celles portant sur l'utilisation des applis pour smartphones, conçues pour permettre aux utilisateurs de gérer leur profil. L'objectif était de répondre à dix questions préalables (voir graphiques ci-dessus) sur les types de données collectées, leur mode d'utilisation et le caractère exhaustif de certaines données. Les informations obtenues ont d'abord été classées en deux séries de données (l'une relative aux politiques de confidentialité pour les services et l'autre pour les applis), puis traduites dans les graphiques ci-dessus. Les parties du texte où se trouvent les réponses aux questions posées ont également été insérées dans les graphiques.

Opérateurs de téléphonie et données à caractère personnel : le contexte européen

Abstract: Cet article est le prolongement de notre analyse de l'utilisation des données personnelles par les compagnies de téléphonie. Il aborde également des questions juridiques liées à la réglementation européenne

Link: https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/Mobile-operators-and-personal-data-in-Europe

Author: Federico Caruso, Gianluca De Feo (OBCT/CCI)

Text:

Lisibilité

Comme indiqué dans plusieurs points du règlement général sur la protection des données (RGPD) - considérants 39, 42, 58 et articles 7, 12 -, les informations relatives au traitement des données à caractère personnel doivent être fournies sous une forme compréhensible et aisément accessible. Or

force est de constater que les entreprises faisant l'objet de notre étude ne font pas de grands efforts en ce sens. À part le « mur de texte » traditionnel, ils ne proposent pas une mise en page, un langage ou des éléments graphiques propices à la lecture. Ce problème n'est évidemment pas circonscrit aux seules entreprises de télécommunication, comme le montrent diverses analyses à grande échelle ainsi que notre expérience quotidienne. Pourtant, des chercheurs universitaires planchent depuis un certain temps sur des systèmes graphiques basés sur des icônes permettant de présenter des informations immédiates. Mais aucun des opérateurs analysés n'a adopté de procédés similaires. Il convient toutefois de faire la distinction entre ceux qui se limitent à publier un texte juridique au format PDF, sans fournir une mise en page soignée ni un langage compréhensible, et ceux qui simplifient la communication, avec une foire aux questions ou des pages ressemblant à de mini-sites web. Mais ils pourraient faire plus, notamment en termes d'homogénéité des politiques de confidentialité entre les différents fournisseurs. Cela favoriserait la transparence en rendant la comparaison plus aisée.

Caractère exhaustif

La politique de confidentialité des données devrait énoncer clairement les droits des utilisateurs : droits d'accès, de rectification et d'effacement des données, droits de limitation et d'opposition au traitement des données, droit au retrait du consentement donné et droit d'introduire une réclamation. Dans son rapport sur les logiciels de vidéoconférence, NOYB évoque les lignes directrices du groupe de travail « article 29 » sur la protection des données, selon lesquelles le responsable du traitement ne devrait pas se limiter à informer de l'existence de tels droits, mais inclure également « un résumé de ce que comprend le droit en question et des mesures pouvant être prises par la personne concernée pour l'exercer, ainsi que toute limitation audit droit ». Cette question fait l'objet de diverses approches. Les informations sont souvent partielles et les droits décrits de façon très synthétique, parfois sans même indiquer les coordonnées de la personne ou du bureau chargé de recevoir les demandes. Mentionnons à cet égard le cas de l'appli de Vodafone Allemagne, dont la politique de confidentialité ne contient aucune référence à ces droits. En Italie, certaines entreprises optent plutôt pour des formules vagues, comme « Vous avez le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente en matière de protection des données à caractère personnel » (Tim et sa filiale Kena Mobile), mais sans en préciser les modalités ni la base juridique sur laquelle elle pourrait se fonder.

Les catégories de données collectées et leur traitement

En ce qui concerne les types de données prises en compte dans la présente étude, le tableau est assez homogène entre les différents pays. La tendance générale consiste à collecter les données de position, de navigation et de comportement de l'utilisateur. En général, le consentement de ce dernier constitue la base juridique à cette fin, bien que certains opérateurs se limitent à invoquer l'existence d'un intérêt légitime. En revanche, plusieurs situations se présentent à l'égard des données biométriques. Il n'est souvent pas indiqué si ces dernières sont collectées ou non, mais cela peut être dû au fait qu'elles sont

incluses dans les autres catégories citées. Leur définition comporte d'ailleurs des caractéristiques communes aux données comportementales, comme le rythme de frappe ou de défilement sur l'écran. D'autres éléments biométriques présents dans les smartphones de dernière génération, comme la reconnaissance des empreintes digitales ou la reconnaissance faciale, devraient toutefois faire l'objet d'une mention spéciale.

Vis-à-vis des activités de profilage - analyse des données en vue d'améliorer le service ou de proposer des offres commerciales « sur mesure »-, le consentement explicite de l'utilisateur semble être la donne générale. Mais certains opérateurs, comme Orange et Vodafone en Espagne, indiquent que le profilage sera réalisé dans tous les cas. C'est un peu plus flou, en revanche, pour Vodafone et Congstar GmbH en Allemagne (et, en partie, Digi et l'appli de Yoigo en Espagne) : d'après les informations que nous avons pu recueillir, aucun d'entre eux n'indique explicitement les catégories de données collectées ni si elles feront l'objet d'un profilage.

Cession et effacement des données

Tous les opérateurs déclarent que les données à caractère personnel seront cédées sous certaines conditions à des tiers. Ces derniers sont chargés, dans la plupart des cas, de mettre en œuvre des activités liées à l'exécution du contrat ou à l'évaluation de la solvabilité du client. Il arrive que des partenaires commerciaux – pouvant appartenir au même groupe d'entreprises que l'opérateur - soient directement nommés : les données pourront leur être cédées, avec le consentement de l'utilisateur, à des fins très diverses, y compris l'envoi de messages proposant des biens ou des services sans aucun rapport avec la téléphonie. Les formules employées sont parfois très générales, surtout dans le cas des services proposés par les fournisseurs français (Orange, Bouygues Telecom) et allemands (Vodafone, O2, Congstar GmbH). Il en va de même concernant leurs applis, ainsi que celles de Yoigo (Espagne) et de Telekom, Aldi Talk et 1&1 Telecom GmbH (Allemagne).

En ce qui concerne la conservation des données, certaines sociétés informent en quelques lignes seulement que ces dernières seront conservées « pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont collectées ou traitées ultérieurement » (Tim Italia). Elles fixent également un délai maximal au-delà duquel elles seront effacées. D'autres, en revanche, font preuve de plus de transparence et publient un tableau illustrant en détail les durées de conservation selon les catégories (Coop voce, ho., Vodafone et Wind Tre en Italie ; Bouygues Telecom en France). En Allemagne, les données sont généralement effacées dans un délai de 12 à 14 mois.

RGPD

Les articles 13 et 15 du RGPD sont les plus pertinents dans le cadre de notre étude. Comme l'explique Stefano Rossetti, avocat au sein de l'organisation noyb.eu, ils régissent les deux « moments clés »

dans les relations entre l'utilisateur et l'opérateur à l'égard du traitement des données à caractère personnel.

L'article 13 énumère l'ensemble des informations que l'entreprise doit fournir au premier de ces deux moments clés, à savoir la souscription d'un service. Comme indiqué dans le rapport susmentionné de NOYB, ces informations figurent habituellement dans un document appelé « politique de confidentialité » (l'objet principal de notre analyse). Ce dernier doit toujours comporter trois éléments : les *catégories* de données collectées, les *finalités* pour lesquelles elles sont requises et la *base juridique* de leur traitement. Parmi les autres renseignements à fournir, mentionnons l'identité et les coordonnées du responsable du traitement, les destinataires éventuels des données (pouvoirs publics, autres entreprises, etc.), leur durée de conservation, l'existence du droit de demander l'accès aux données ou l'effacement de celles-ci et le droit d'introduire une réclamation en cas de violation des dispositions.

Concernant le caractère exhaustif des informations fournies, les nouvelles lignes directrices sur le droit d'accès aux données, en cours d'élaboration par l'EDPB (Comité européen de la protection des données), semblent laisser une certaine marge de manœuvre au responsable du traitement : « les informations [sur le traitement et les droits des personnes concernées] peuvent s'appuyer sur celles du registre des activités de traitement du responsable à cet égard (art. 30) et sur celles figurant dans la politique de confidentialité (art. 13 et 14). Ces informations d'ordre général devront toutefois être mises à jour au moment de la demande, ou adaptées aux opérations de traitement mises en œuvre pour la personne concernée ».

Cela nous conduit au deuxième « moment clé » des relations entre utilisateurs et opérateurs, comme indiqué à l'article 15 : « La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel ». Alors que l'article 13 stipule que l'entreprise est tenue d'informer l'utilisateur (en indiquant la marche à suivre), l'article 15 précise qu'il lui incombe également de répondre à toute demande d'accès de ce dernier à ses données, afin de pouvoir vérifier si les données collectées et leur traitement sont conformes aux dispositions de la politique de confidentialité ainsi qu'à la loi. Dans le cadre de ce travail, nous nous sommes limités à la première partie.

2. La stratégie européenne de cybersécurité

Le plan de Bruxelles pour protéger l'UE contre les cyberattaques

Abstract: La crise sanitaire du COVID-19 nous a fait entrer de plain-pied dans la société numérique. Une grande partie des activités de la vie quotidienne se déroule maintenant dans la sphère numérique, ce qui fait que les États membres sont désormais plus exposés aux cyberattaques. Pour les prévenir, la Commission européenne a lancé sa nouvelle stratégie de cybersécurité en décembre 2020.

Author: Álvaro Merino (El Orden Mundial)

Link: https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/Brussel-s-plan-to-protect-the-EU-from-cyberattacks

Text:
« Qui êtes-vous ? Vous participez à notre réunion. Mon général, que devons-nous faire, selon vous ? Mon général, vous avez raison : nous devons investir dans la protection de la confidentialité ». C'est de cette manière que Josep Borrell, le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité, a réagi lorsqu'une vidéoconférence secrète des ministres de la défense de l'UE a été piratée l'année dernière. Par inadvertance, le ministre néerlandais de la défense avait partagé sur Twitter une photo sur laquelle figurait le code d'accès à la réunion. Un journaliste compatriote de ce ministre, a mis à profit cette erreur pour s'inviter à la conférence, mettant ainsi dans l'embarras cette vénérable institution.

Cette anecdote – aussi extravagante soit-elle – met en évidence les difficultés que connaît actuellement l'UE en matière de sécurité : dans un club qui fédère 27 membres, dont les réunions et les conversations devraient avoir idéalement lieu en présence directe, mais qui se déroulent en ligne pour des raisons de difficultés logistiques, il est difficile de s'assurer que les portes restent bien closes.

Dans un monde connecté comme le nôtre, c'est l'imminence de ce risque considérable qui a contraint l'UE à s'armer contre les attaques numériques, quel que soit le moment où elles se produisent, quelle que soit leur cause et quelle que soit la forme qu'elles prennent.

La menace est silencieuse, mais elle n'est pas invisible. Ce n'est pas sans motif valable que l'Agence de l'Union européenne pour la cybersécurité (ENISA) a recensé trois cent quatre attaques malveillantes graves contre des secteurs essentiels en 2020, soit plus du double par rapport à 2019. Nombre d'entre elles ont visé des hôpitaux et des réseaux de santé, des établissements qui, pendant la durée de la pandémie, détenaient des informations très précieuses sur l'évolution de la pandémie de COVID-19 et les futurs projets de vaccination.

Leurs objectifs peuvent être divers, du vol de données à la paralysie d'infrastructures cruciales, avec les conséquences désastreuses que cela représente pour le pays concerné. L'exemple récent le plus marquant est la cyberattaque de Colonial Pipeline, le plus grand oléoduc des États-Unis qui a eu lieu au mois de mai 2021. Cette attaque, perpétrée par un groupe apolitique de hackers professionnels dénommé Darkside, a contraint les exploitants à interrompre le flux de pétrole, ce qui a causé une

pénurie d'essence sur toute la côte est, et à verser au groupe une somme de 75 bitcoins, soit l'équivalent de 3,8 millions d'euros.

Heureusement pour les citoyens européens, l'UE a un plan pour faire en sorte que le piratage d'une réunion secrète de la défense reste dans les mémoires davantage comme une anecdote amusante que comme une cyberattaque mettant en péril l'ensemble de la sécurité de l'Europe. En décembre 2020, la Commission européenne a présenté une nouvelle stratégie de cybersécurité et une proposition de renforcer la directive relative aux mesures destinées à assurer un niveau élevé commun de sécurité dans l'Union (directive SRI 2).

Une nouvelle course aux armements

L'Union européenne se prépare depuis 2013 à riposter aux attaques. Dernièrement, elle a lancé plusieurs initiatives pour instaurer une stratégie commune de défense et de sécurité.

Parmi celles-ci il convient de mentionner une boîte à outils cyberdiplomatique commune et un cadre stratégique de cyberdéfense de l'UE, toutes les deux adoptés en 2018 et destinés à améliorer la coordination entre les États membres ; la loi sur la cybersécurité (2019) qui a renouvelé le mandat de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) rebaptisée Agence européenne de l'Union européenne pour la cybersécurité ; et la boîte à outils européenne pour la sécurité des réseaux 5G, également en 2019.

Pourtant, dans un monde hyperconnecté comme le nôtre, où les menaces hybrides sont de plus en plus sophistiquées et où les grandes puissances rivalisent pour développer des technologies leur permettant de sécuriser leurs systèmes, le risque d'être distancé dans la cybercourse est de plus en plus grand. De ce point de vue, la course à la cybersécurité fait penser à la course aux armements de la Guerre froide quand les États-Unis, l'Union soviétique et leurs alliés respectifs se sont engagés dans une guerre secrète de développement d'armes nucléaires. Comme aujourd'hui, chaque avancée était jalousement gardée et les progrès accomplis obligeaient chaque partie à avancer de plus en plus vite.

C'est ce qui contraint l'Union européenne à moderniser continuellement sa stratégie de cybersécurité pour garder une longueur d'avance sur les cybercriminels. C'est la raison pour laquelle, même si le document a été publié pour la première fois en 2013, la stratégie a été révisée en 2017, puis en décembre 2020.

Quoi qu'il en soit, la version la plus récente constitue un changement de paradigme : désormais les institutions européennes et les États membres peuvent compter sur des mesures de sécurité unifiées et coordonnées, l'UE veut créer des outils qui lui permettent de réagir immédiatement et efficacement ou – mieux encore – de prévenir les cyberattaques.

Un plan ambitieux

À cet égard, la nouvelle stratégie de cybersécurité implique trois domaines cruciaux : tout d'abord, elle vise à améliorer la résilience commune face aux cyberattaques à la fois par la création d'un réseau de centres d'opérations de sécurité dans toute l'UE qui travaillent avec des technologies d'intelligence artificielle et par une réforme des lois de sécurité relatives aux réseaux et systèmes d'information intégrée à la directive SRI 2.

La directive SRI, adoptée en 2016, a provoqué un changement dans l'orientation institutionnelle de la cybersécurité au sein des États membres en les obligeant notamment à créer une stratégie nationale de cybersécurité et à mettre en place des équipes de cyberintervention d'urgence, même si elle a commencé à montrer ses limites.

« La transformation numérique de la société, intensifiée par la crise de la COVID a augmenté le niveau de menace et lance de nouveaux défis qui nécessitent de fournir des réponses innovantes et adaptées. Désormais, chaque attaque peut avoir des effets d'une grande ampleur sur tout le marché intérieur. » Tels sont les mots prononcés par la Commission européenne lors de la présentation de sa nouvelle stratégie.

En bref, la directive SRI 2, qui a reçu le feu vert du Parlement européen en octobre, élargit la définition de la notion de secteurs essentiels et renforce les exigences pour les 160 000 entreprises qui exercent leurs activités dans ces secteurs. L'objectif est de combler le fossé existant entre les entreprises européennes et américaines, ces dernières investissant, en moyenne, 41% de plus, dans la cybersécurité que leurs homologues européennes.

Deuxièmement, avec sa nouvelle stratégie en matière de cybersécurité, la Commission souhaite également renforcer sa capacité opérationnelle à prévenir, dissuader et répondre aux cyberattaques, ce qui a abouti à la proposition de créer une unité conjointe de cybercriminalité. Cette équipe s'efforcera de fournir une réponse coordonnée de l'UE aux cyberincidents et aux cybercrises à grande échelle et d'offrir une aide pour rétablir une situation normale après ces attaques. « Ces menaces constituent un ennemi commun, c'est pourquoi il est nécessaire de se coordonner, de partager les renseignements et de donner l'alerte rapidement », argumente la Commission.

Enfin, Bruxelles veut promouvoir un cyberespace mondial et ouvert en faisant venir à la table les pays extérieurs pour reproduire ses lois dans le monde entier et contribuer à la sécurité mondiale. En d'autres termes, la stratégie vise à éviter que le visage de la cybersécurité ne rappelle celui de la Guerre froide en rassemblant les pays dans un esprit de coopération pour protéger le monde contre les menaces de ce type.

L'AESRI, garante de la stratégie commune de cybersécurité de l'UE

Abstract: L'agence en charge de la cybersécurité a la mission d'ériger un système de défense commun contre les attaques cybernétiques au sein de l'Union européenne. Malgré de modestes

prétentions initiales, elle a réussi, réforme après réforme, à devenir le fer de lance de l'UE contre les cybercriminels.

Author: Álvaro Merino (El Orden Mundial)

Link: https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/ENISA-The-cornerstone-of-the-EU-s-cybersecurity-strategy

Text:

L'Agence européenne chargée de la sécurité des réseaux et de l'information (AESRI) a été fondée en 2004. Facebook n'en était alors qu'à ses débuts et le préfixe « cyber » relevait de la science-fiction. Créée initialement pour une durée de cinq ans, la Commission européenne a prolongé plusieurs fois son mandat jusqu'à en faire une agence permanente en 2019. En outre, son siège est situé à Héraklion et à Athènes, en Grèce, aux antipodes de Bruxelles.

En dépit de ce contexte peu prometteur, l'AESRI a réussi à s'imposer comme un facteur de cohésion de la stratégie de cybersécurité européenne. Preuve en est sa nouvelle appellation après la dernière refonte : « Agence de l'Union européenne pour la cybersécurité » (son acronyme AESRI demeurant en l'état). Elle a désormais pour mission de « parvenir à un niveau commun élevé de cybersécurité dans l'ensemble de l'Union, y compris en aidant activement les États membres et les institutions, organes et organismes de l'Union ».

C'est donc à cette agence qu'a été confiée la tâche d'assurer la sécurité des réseaux et de l'information de l'Union européenne. En proposant sa création, la Commission visait en effet à mettre en place un organe de supervision chargé de combler les failles de sécurité tout en veillant à ce que toutes les directives soient mises en œuvre. Sans ce niveau de protection harmonisée, l'UE serait une cible facile pour les cybercriminels. En outre, l'agence collabore étroitement avec Europol et le Centre européen de la cybercriminalité.

En 2004, cette initiative ne faisait qu'anticiper l'importance qu'Internet allait prendre progressivement dans la vie quotidienne des citoyens. À mesure que se développaient les technologies de l'information et de la communication (TIC), les risques qui leur étaient liés augmentaient de façon exponentielle. Se protéger contre ces menaces ne relevait donc plus d'une démarche visionnaire, mais devenait une véritable obligation. L'Agence européenne pour la cybersécurité y a fait face avec brio et rigueur.

Sans l'AESRI, les cyberattaques seraient beaucoup plus fréquentes. Certaines arrivent toutefois à passer entre les mailles du filet, comme celle qui a frappé l'Hôpital universitaire de Brno (République tchèque) en mars 2020, en pleine pandémie. Suite à cette agression, les opérations urgentes ont dû être reportées et les patients graves ont été transférés dans d'autres services. La pandémie a rendu les choses plus difficiles, les menaces se multipliant au même rythme que le développement frénétique de la transformation numérique de la société et de l'économie. Des services d'approvisionnement en eau

aux systèmes de surveillance du domicile, notre monde est de plus en plus connecté. Le corollaire est que le champ d'action des cybercriminels connaît de moins en moins de limites.

Une ascension progressive

Agence modeste au départ, l'AESRI avait une mission très précise : aider les institutions et les organisations de l'Union européenne à sécuriser leurs connexions. En 2008, un an avant l'expiration de son premier mandat, le Parlement et le Conseil européen, sur proposition de la Commission, ont décidé d'en prolonger la durée jusqu'en 2012, dans la mesure où le processus d'évaluation et d'amélioration de la protection des réseaux européens ne faisait que débuter.

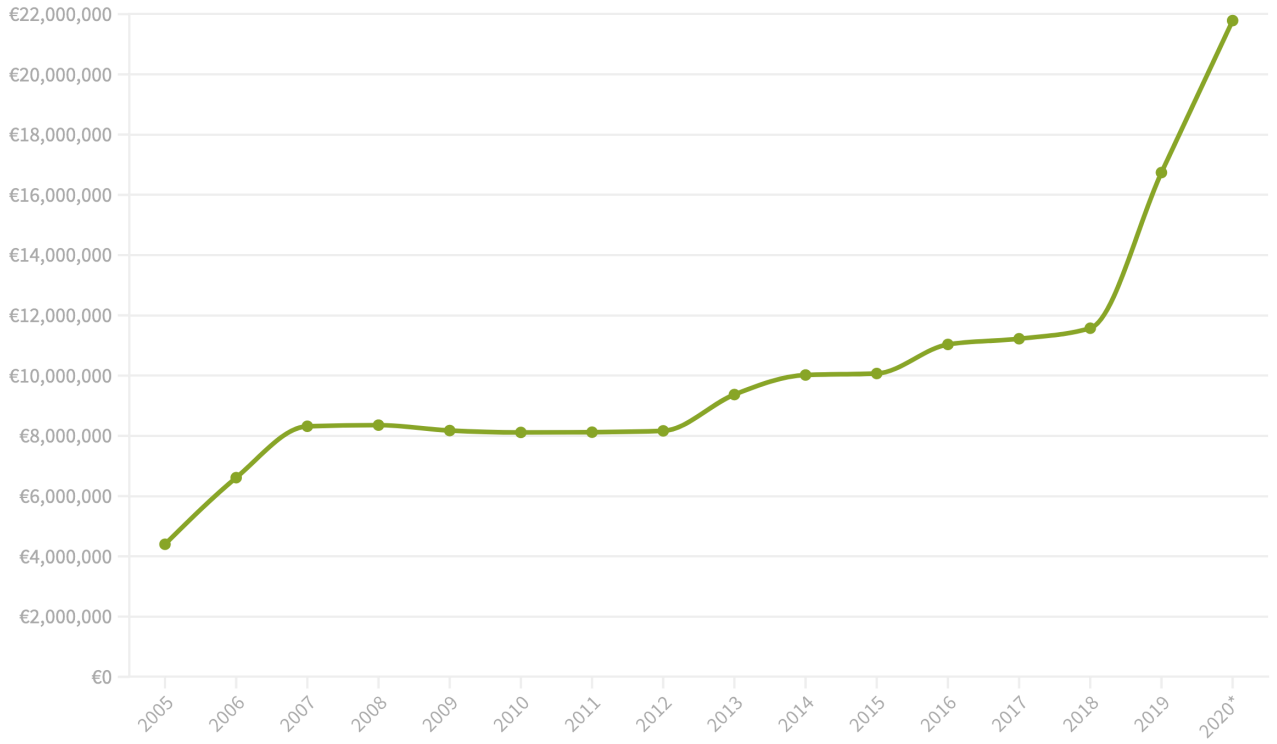
En 2011, son mandat a été prolongé jusqu'en 2013, puis à nouveau jusqu'en 2020. Contrairement aux prolongations précédentes, cette dernière s'est accompagnée d'un élargissement de ses compétences. À l'occasion de la publication de la première stratégie de cybersécurité de l'UE, les institutions communautaires ont plaidé pour la modernisation de l'agence. Parmi ses nouvelles fonctions, mentionnons la coordination de la future équipe d'intervention en cas d'urgence informatique (EU CERT), répartie dans tous les États membres.

Mais c'est en 2019, suite à l'entrée en vigueur du règlement sur la cybersécurité, que l'AESRI a définitivement reçu ses lettres de noblesse : appelée désormais l'« Agence de l'Union européenne pour la cybersécurité », ses ressources ont augmenté et son mandat a été prolongé indéfiniment. Son rôle consultatif a été étendu et des tâches opérationnelles précises lui ont été confiées pour la première fois.

C'est ainsi qu'elle a commencé à aider les États membres à établir des priorités en matière d'investissement en recherche et développement et, surtout, à développer un système de certificats de sécurité pour les produits et services TIC dans l'Union.

Des dispositifs sécurisés sont nécessaires pour que les entreprises et les consommateurs aient l'assurance que leurs données en ligne sont bien protégées. Un système de certification unique s'avère donc indispensable pour renforcer leur confiance et stimuler le commerce frontalier. À cette fin, l'AESRI doit établir des critères communs et harmoniser les mécanismes nationaux afin de délivrer des certificats de cybersécurité pour les cartes intelligentes (cartes de crédit, de transport, SIM...), les services d'informatique en nuage, etc.
Sur le plan financier, l'agence a vu son enveloppe augmenter d'année en année, atteignant près de 22 millions d'euros en 2020, soit cinq plus que son budget initial. La plupart des fonds proviennent de la Commission européenne, auxquels s'ajoute une contribution plus modeste des États de l'Association européenne de libre-échange, non membres de l'UE - Islande, Liechtenstein, Norvège et Suisse – et du gouvernement grec (qui prend en charge la location des installations). Elle employait 75 personnes en 2019.

Le budget de l'AESRI a fortement augmenté



Source: Comptes annuels de l'AESRI • Álvaro Merino
*Le montant de 2020 est provisoire

EUROPEAN DATA JOURNALISM NETWORK

L'importance croissante de l'AESRI dans la stratégie de cybersécurité de l'UE a incité la Commission européenne à la rapprocher de sa sphère d'influence. Au lieu de changer son siège, elle a donc autorisé en juin dernier l'établissement d'un troisième bureau local à Bruxelles, afin que l'agence maintienne « une coopération régulière et systématique » avec les institutions européennes.

Petit à petit, l'Agence européenne chargée de la sécurité des réseaux et de l'information s'est donc imposée comme le pilier de la cybersécurité européenne. Son installation à Bruxelles et la consolidation de ses fonctions opérationnelles marqueront l'aboutissement d'un processus qui s'inscrit dans la volonté de l'Union de passer à l'offensive contre les attaques cybernétiques et de contrer les desseins des cybercriminels du monde entier.

Cybersécurité : coordination européenne et agences nationales

Abstract: Les agences européennes jouent un rôle de soutien et de coordination de la cybersécurité européenne. Cependant, en se basant sur les réglementations spécifiques de l'UE, chaque État membre peut créer ses propres structures aussi bien pour le secteur privé que le secteur public, ce dernier occupant une place prépondérante en la matière.

Author: Openpolis

Link: https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/Cybersecurity-between-European-coordination-and-national-agencies

Text:

Ces dernières années, l'Agence européenne pour la cybersécurité (ENISA) est devenue un acteur de plus en plus important *pour résoudre les défis croissants dans ce secteur. La compétence de l'Union européenne dans le domaine de la cybersécurité résulte de l'article 5 du traité sur l'Union européenne (TUE), qui prévoit une compétence partagée dans les domaines où il n'y a pas de compétence exclusive.*

En vertu du principe de subsidiarité, dans les domaines qui ne relèvent pas de sa compétence exclusive, l'Union intervient seulement si, et dans la mesure où, les objectifs de l'action envisagée ne peuvent pas être atteints de manière suffisante par les États membres, tant au niveau central qu'au niveau régional et local, mais peuvent l'être mieux, en raison des dimensions ou des effets de l'action envisagée, au niveau de l'Union. (TEU Art 5.3)

L'UE (et par extension l'ENISA) doit donc limiter son action aux questions qui ne peuvent être résolues par les États membres de façon individuelle. C'est pourquoi, en plus de cette agence européenne, chaque État membre a adopté son propre cadre institutionnel et ses propres instances chargées de la cybersécurité. La mission de l'ENISA est donc de soutenir les États membres et la Commission et de faciliter la coopération et l'échange d'informations.

Coordination européenne

Alors que la principale référence réglementaire concernant la cybersécurité européenne est actuellement la directive SRI EUR-Lex - 32016L1148 - EN - EUR-Lex (europa.eu), une mise à jour du texte est en cours de discussion et doit aboutir à l'acceptation de la directive SRI 2.

En considérant la nature intrinsèque des directives européennes (article 288 du traité sur le fonctionnement de l'Union européenne, TFEU) le texte se borne à indiquer aux États membres les résultats souhaités, en leur laissant une large autonomie pour organiser leurs propres agences de cybersécurité.

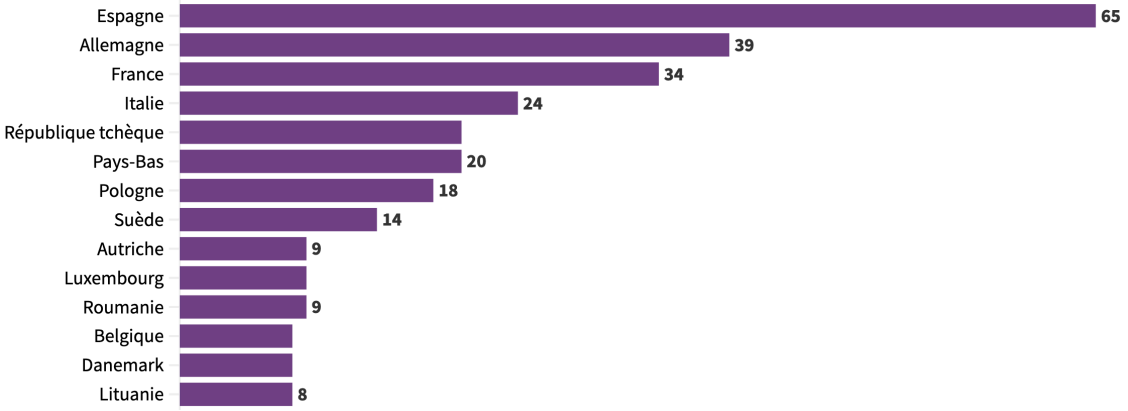
Parmi les obligations imposées aux États membres figure l'identification d'agences spécifiques qui coordonnent les mesures adoptées pour assurer un niveau élevé de cybersécurité. Il s'agit des autorités nationales compétentes, des points de contact uniques et des CSIRT (Computer Security Incident Response Team).

Déjà établis en 1990, les CSIRT sont des organisations chargées de collecter et de gérer les rapports d'incidents et de vulnérabilités potentielles des logiciels. Chaque pays a un nombre différent de CSIRTs qui peuvent être accrédités par divers consortiums internationaux tels que Trusted Introducer,

First (Forum regroupant les Équipes de sécurité et d'intervention) et le Réseau Européen CSIRT Network.

Les 15 premiers pays de l'UE par nombre de CSIRT

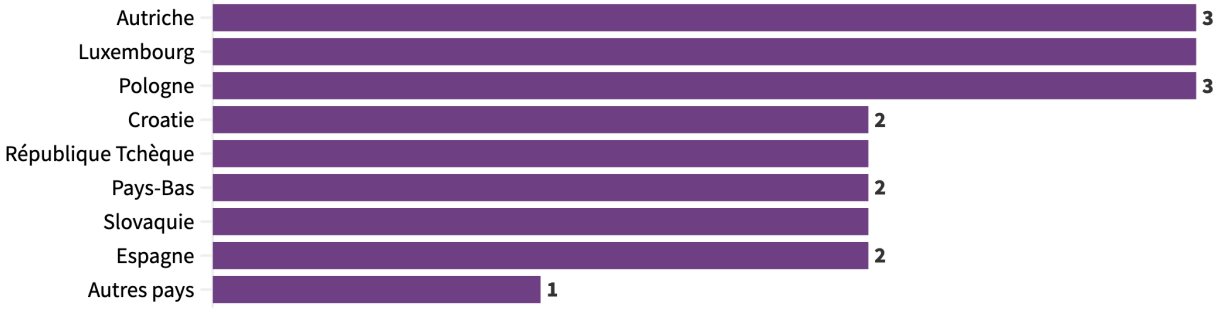
Les pays européens comptant le plus grand nombre d'équipes de réponse aux incidents de sécurité informatique (CSIRT) accréditées par les trois principaux consortiums internationaux



La directive SRI oblige chaque État membre à désigner un ou plusieurs CSIRT pour rejoindre le réseau européen des CSIRT. Dans la plupart des cas, les États membres ont désigné un seul CSIRT, mais pas tous. En effet, certains pays en ont désigné deux ou trois.

CSIRT nationaux désignés par les pays membres

Nombre de CSIRT nationaux désignés par chaque pays membre de l'Union européenne comme faisant partie du réseau CSIRTs.



Alors que les CSIRTs s'occupent des incidents informatiques et des vulnérabilités potentielles, les autorités compétentes des SRI opèrent au niveau de la réglementation et de la gestion. Il s'agit des organismes nationaux responsables de la sécurité des réseaux et des systèmes d'information dans les secteurs indiqués dans la directive. Dans ce cas également, chaque État peut désigner un ou plusieurs organismes compétents.

13 pays ont désigné une seule autorité compétente en matière de SRI.

Si une seule autorité est identifiée, elle devient automatiquement le point de contact unique. Dans le cas contraire, l'État doit indiquer quel organisme jouera le rôle de liaison pour assurer la coopération avec les autorités des autres États membres ainsi qu'avec l'ENISA et le réseau CSIRT.

Les autorités compétentes en matière de SRI : un regard sur l'Allemagne, la France et l'Italie

Comme nous l'avons vu, chaque pays a le droit de structurer ses propres organismes compétents comme il l'entend, dès lors qu'il respecte les obligations de la directive européenne. Si l'on prend l'exemple des trois pays les plus peuplés de l'UE, le premier fait qui ressort est que tous trois, à ce jour, ont identifié une seule autorité SRI.

Dans le cas de l'Italie, l'unique autorité SRI est la nouvelle agence de cybersécurité. Avant la création de cette agence en mai 2021, il existait cinq autorités désignées, à savoir les ministères du développement économique, des infrastructures, de l'économie, de la santé et de l'environnement, désormais définis comme des « autorités sectorielles » (article 7 du décret législatif 65/2018).
L'Agence de cybersécurité représente donc le point de contact unique, tout en contenant également le CSIRT italien, qui était auparavant inclus dans le département de l'information pour la sécurité de la république (relevant ainsi de la rubrique du renseignement).

Comme nous l'avons expliqué dans d'autres articles, l'Agence de cybersécurité est, à bien des égards, autonome. Elle est toutefois placée sous la tutelle de la présidence du Conseil, qui supervise la gestion du secteur ainsi que la nomination du directeur (Roberto Baldoni) et du vice-directeur (Nunzia Ciardi). En interne, l'agence est structurée en huit services généraux, subdivisés à leur tour en divisions. Actuellement, l'effectif envisagé devrait atteindre un maximum d'environ 300 personnes, pour un budget de 41 millions d'euros pour 2022. Cependant, une forte augmentation des ressources est attendue pour les prochaines années.

Un budget de 122 millions d'euros est planifié à partir de 2026 pour l'agence italienne de cybersécurité.

En France, l'autorité compétente est l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Comme en Italie, l'agence dépend du Premier ministre. Plus précisément, l'agence française fait partie du Secrétariat général de la défense, un organisme spécifique qui assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.
Créée par la loi en 2009, l'ANSSI s'est immédiatement fixé des objectifs ambitieux, dont celui de devenir un leader mondial de la cybersécurité. Cette formulation n'est plus présente dans la version la plus récente de la stratégie française en matière de cybersécurité.
L'ANSSI est chapeautée par une direction générale à la tête de laquelle siège le directeur général, Guillaume Poupard, ainsi que le directeur général adjoint et le chef de cabinet. Au niveau inférieur, on trouve quatre sous-directions composées de plusieurs divisions. Hors masse salariale, le budget de l'ANSSI s'élevait, en 2020, à environ 21 millions d'euros, pour un personnel qui comptait plus de 500 agents et 100 personnes en cours de recrutement.

L'ANSSI dispose d'un budget de 21 millions d'euros, hors coûts de personnel.

L'Allemagne est également dotée d'une autorité compétente unique : l'Office fédéral de la sécurité des technologies de l'information (BSI). Contrairement à ce qui se passe en France ou en Italie, cet organisme n'est pas placé sous l'autorité du Premier ministre (le chancelier, en l'occurrence), mais il fait partie de la Direction générale de la cybersécurité et de la sécurité de l'information du ministère de l'intérieur. L'office a été créé en 1991, mais aujourd'hui ses attributions sont principalement régulées par une loi de 2009. Des mesures ultérieures ont ensuite été adoptées : la première en 2015 a anticipé de nombreux éléments de la directive européenne publiée l'année suivante, la deuxième il y a seulement quelques mois. Avec cette dernière législation, le gouvernement allemand entend renforcer davantage le BSI, notamment en matière de protection des consommateurs, de sécurité des entreprises et des réseaux de téléphonie cellulaire.

Le BSI est dirigé par un président, Arne Schönbohm, et par un vice-président. L'office fédère huit divisions, elles-mêmes regroupant 18 branches et plusieurs sections. En 2021, son budget s'est élevé à 200 millions d'euros, pour un effectif de 1 550 personnes.

En 2021, le budget de l'Office fédéral allemand de la sécurité des technologies de l'information s'est élevé à 200 millions d'euros

Les informations relatives aux budgets et aux effectifs de ces organismes – aussi intéressantes soient-elles – sont difficilement comparables. Cela s'explique par la diversité des sources et les méthodologies utilisées, mais aussi par le fait que, dans aucun de ces pays, la cybersécurité ne relève d'une seule organisation. Différentes structures, comme les ministères, les institutions de défense et les services de renseignement jouent un rôle important dans ce domaine et il est donc difficile d'évaluer les efforts effectués respectivement par chaque pays en matière de cybersécurité.

La relation entre le secteur de la défense et le renseignement

Comme mentionné plus haut, avant la naissance de l'Agence italienne de cybersécurité, cette compétence était du ressort du Département de l'information pour la sécurité de la république (DIS). La nouvelle loi a toutefois fait sortir l'agence du domaine de compétence du renseignement, même si de nombreux liens subsistent entre les deux secteurs. Par ailleurs, la coordination avec le sous-secrétaire d'État chargé du renseignement est assurée par la présence de représentants des agences de renseignement au cœur du système de cybersécurité dont font également partie les représentants de divers ministères. La présence d'un représentant du ministère de la défense est également prévue, ce qui garantit le lien entre l'agence et Network Operations Command (COR), l'organe de cybersécurité placé sous le commandement du chef d'État-Major des armées. Dans les réglementations publiées jusqu'à présent, il n'existe cependant pas de lien explicite entre l'agence et le COR.

L'Office fédéral allemand de la sécurité des technologies de l'information trouve également son origine dans les services du renseignement. Au début des années 1990, son rôle était assuré par un bureau chargé de la protection technologique des secrets d'État. Au fil des ans, toutefois, le BSI est devenu une institution totalement autonome. Les relations avec la communauté du renseignement sont maintenues par l'intermédiaire de Centre national de cyberdéfense, un organisme interinstitutionnel qui regroupe diverses structures fédérales chargées de la sécurité. Les relations avec l'armée – un secteur qui joue un rôle fondamental en Allemagne – sont également maintenues. La cyberdéfense est, en effet, constitutionnellement attribuée aux forces armées. En 2017, le kommando Cyber -und Informationraum (CIR) a été créé. Cet organe est considéré – au même titre que les autres commandements des forces armées allemandes – comme chargé de la sécurité des infrastructures de cyberdéfense et des systèmes d'armement. Étant donné la relation étroite qui unit la défense et la cybersécurité, le CIR apporte son soutien au BSI en cas de nécessité. Cependant, compte tenu des limites constitutionnelles strictes imposées à l'armée allemande, il ne peut fournir qu'une assistance de nature « administrative ». En effet, lorsqu'il est nécessaire de déployer du personnel militaire en riposte à une cyberattaque d'envergure nationale, une autorisation préalable du parlement est constitutionnellement requise.

Comme nous l'avons vu, en France, l'ANSSI est intégrée au sein du Secrétariat de la défense et de la sécurité nationale. Cette structure garantit la coordination entre le secteur de l'armée et celui du renseignement. En effet, le Secrétariat de la défense et de la sécurité nationale dispose de diverses compétences en matière de défense et de renseignement et confère au président du Conseil des ministres le pouvoir de proposition, de coordination et de régulation des questions générales de défense et de sécurité nationale. En outre, comme nous l'avons vu, le Secrétariat de la défense et de la sécurité nationale est responsable devant le président du Conseil des ministres qui est également responsable des activités des services de renseignement intérieurs et extérieurs, même si ceux-ci relèvent respectivement du ministère de l'intérieur et du ministère de la défense.

Liens :

La protection des données dans l'UE : étude comparative des rapports nationaux. Lire
La cyberdéfense dans les pays de l'OTAN : comparaison des modèles. Lire

La Russie à l'affût de vos données : nette augmentation des cyberattaques au sein de l'Union européenne

Abstract: L'ombre de la Russie a toujours plané au-dessus des réseaux de l'UE. Mais la pandémie de Covid-19, qui a plongé les citoyens dans le monde virtuel, a entraîné des failles de sécurité de plus en plus grandes dans les entreprises et les institutions européennes. Ce n'est pas un hasard si les cyberattaques se sont multipliées en 2020 en Europe. Et bien que Bruxelles fasse tout pour colmater les brèches, l'invasion de l'Ukraine fait redouter une recrudescence de la guerre cybernétique.

Author: Álvaro Merino (El Orden Mundial)

Link: https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/Russia-wants-your-data-cyber-attacks-are-growing-in-the-European-Union

Text:

Atteinte d'une tumeur cérébrale agressive, Donna-Marie Cullen attendait sa séance de radiothérapie le 14 mai 2021, lorsqu'elle a reçu un appel inattendu : le réseau informatique du système de santé irlandais était paralysé suite à une cyberattaque. Son traitement devait être momentanément suspendu. Après une année de lutte acharnée contre le coronavirus, les services de santé irlandais avaient finalement succombé, non pas suite aux contagions ou au chaos généré par le confinement (comme on aurait pu s'y attendre), mais sous l'effet d'une agression invisible commise à des centaines de kilomètres de là.

L'enquête a conclu à un blocage des données causé par un logiciel de rançon (ransonware) activé par Wizard Spider , un groupe cybercriminel basé à Saint-Pétersbourg, en Russie. En échange de l'arrêt de l'attaque, ce groupe réclamait une rançon de quatorze millions de livres - près de dix-sept millions d'euros. Les autorités irlandaises ont décidé de ne pas se plier à leurs exigences, ce qui a entraîné le report de milliers de rendez-vous, le retour du papier et du stylo dans les centres de soins pendant plusieurs mois, la fuite de données médicales confidentielles de 520 patients et des pertes à hauteur de près de cent millions d'euros .

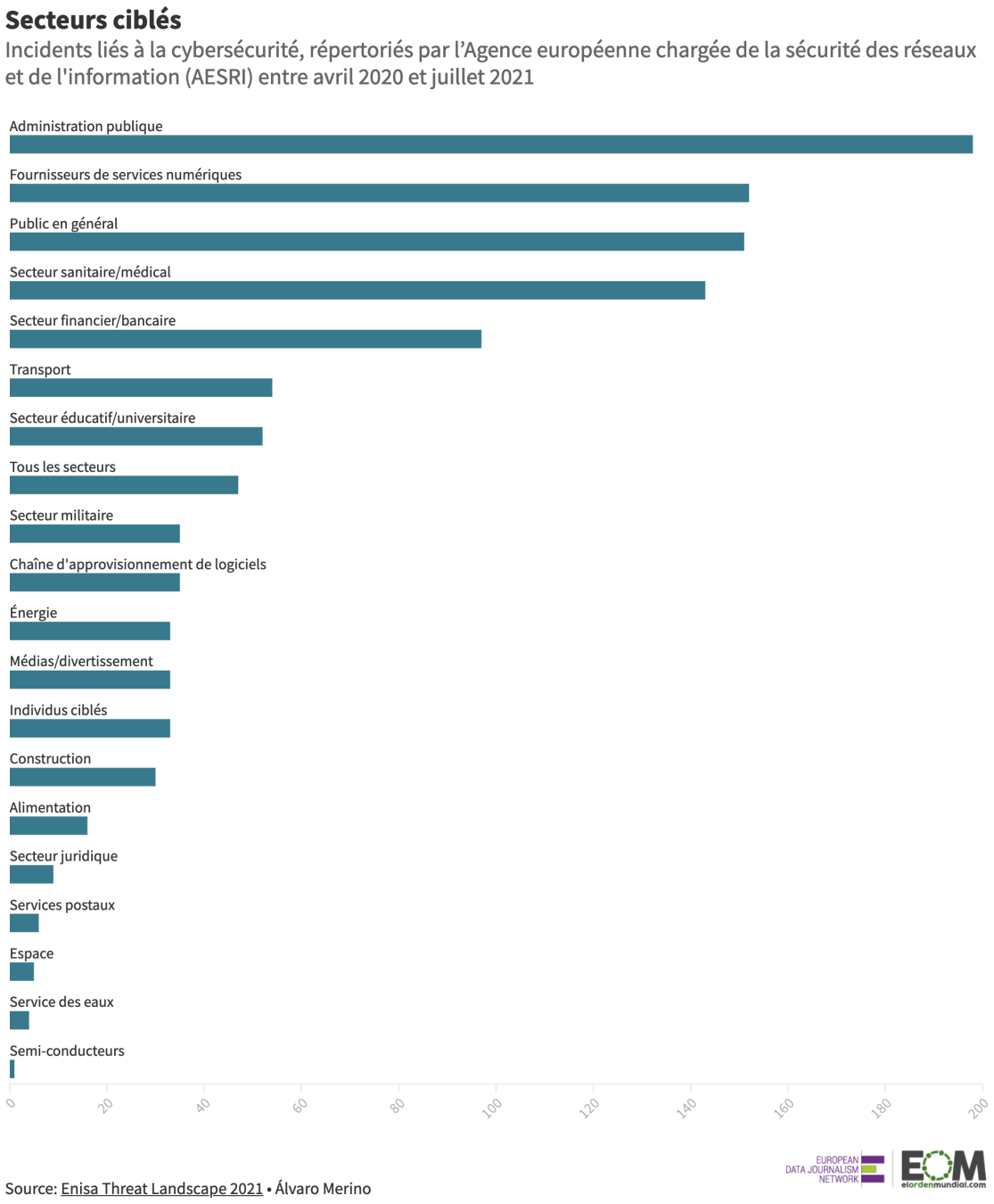
L'agression subie par le service public de santé irlandais est loin d'être un cas isolé. Elle s'inscrit dans une longue série de cyberattaques ciblant les entreprises et les institutions de l'Union européenne. Certes, l'ombre de la Russie a toujours plané au-dessus des réseaux communautaires, mais la fréquence et la virulence de ces attaques n'ont fait qu'augmenter pendant la pandémie.

Ce n'est pas un hasard si les agressions malveillantes contre des secteurs sensibles se sont multipliées en 2020 en Europe (304 attaques, contre 146 en 2019), selon l'Agence européenne chargée de la sécurité des réseaux et de l'information (AESRI). Le nombre d'attaques cybernétiques contre des hôpitaux et des réseaux de soins de santé a également augmenté à hauteur de 47 %.

La « nouvelle normalité », un terreau fertile pour les cybercriminels

Quelques jours à peine après la déclaration de pandémie de COVID-19 par l'OMS, alors que la contagion était hors de contrôle, la vie des Européens a basculé dans l'espace virtuel. Ainsi le télétravail, les achats en ligne et les échanges sociaux par écran interposé sont soudainement devenus la norme. Mais tandis que les solutions numériques permettaient au monde de continuer à tourner et aux entreprises de fonctionner tant bien que mal, elles ont aussi laissé la porte grande ouverte aux activités délictuelles des cybercriminels.

Au-delà de la question de la pandémie, le passage des infrastructures traditionnelles aux plateformes en nuage, l'interconnectivité croissante et l'apparition de nouvelles technologies, comme l'intelligence artificielle, ont renforcé « la sophistication, la complexité et l'impact » des cyberattaques, selon l'AESRI. Dans son rapport de 2021 , cette dernière a indiqué que l'accélération de la transformation numérique « avait augmenté la surface d'attaque, entraînant une hausse du nombre d'agressions cybernétiques contre les bureaux d'organisations et d'entreprises. »



Depuis le déclenchement de la pandémie, l'administration publique, les chaînes logistiques – susceptibles de provoquer des effets en cascade - et les réseaux de santé sont devenus des cibles prioritaires pour les criminels cybernétiques. C'est ainsi qu'en mars 2020, l'hôpital universitaire de Brno , en République tchèque, a également été touché par une attaque qui a eu un impact direct sur ses activités. Son réseau informatique a dû être suspendu, les opérations urgentes ont été reportées et les patients graves transférés dans d'autres services. Même les institutions européennes ont fait l'objet d'une cyberattaque en mars 2021 , bien que sans faille de sécurité apparente.

La Russie, une menace permanente

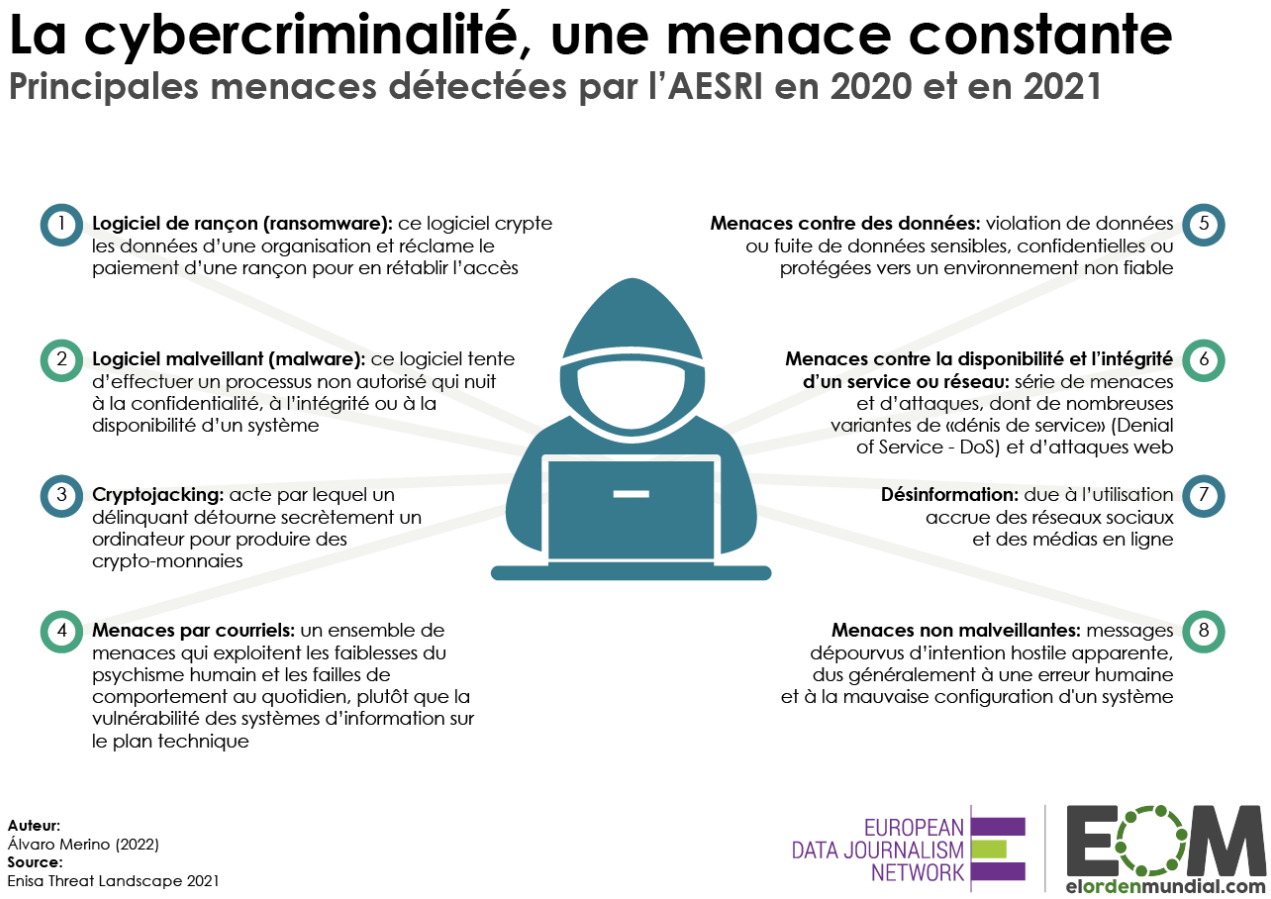
L'anonymat qui caractérise ce type d'agressions rend difficile l'identification de l'ennemi et la mise en place d'une réaction proportionnée. C'est d'autant plus vrai face à la prolifération de groupes non

étatiques derrière lesquels se cachent des dirigeants qui, en public, n'hésitent pas à condamner de tels actes.

Il n'est guère aisé de déterminer précisément la capacité de chaque pays à lancer des attaques cybernétiques. Mais une chose est sûre : la Russie est l'un des acteurs les plus prolifiques dans ce domaine au niveau international. Moscou, en effet, se sert du cyberespace pour renforcer son rôle de puissance mondiale, consolider sa sphère d'influence ou déstabiliser et affaiblir des organisations perçues comme ennemies, l'UE et l'OTAN en particulier.

Les exemples se comptent par dizaines : ces dernières années, l'Allemagne, l'Italie, les Pays-Bas et le Danemark ont affirmé être victimes d'actes de cyberespionnage russe. Début 2021 , la France a informé que plusieurs de ses sociétés, dont Airbus et Orange, avaient subi des attaques de hackers liés à la Russie. En septembre 2021, Josep Borrell, Haut représentant de l'Union européenne pour les affaires étrangères, a accusé Moscou de tentative d'intrusion dans les ordinateurs de nombreux responsables politiques européens, de journalistes, de hauts cadres d'entreprises énergétiques et de certaines personnalités.

Outre des informations sensibles, les cybercriminels russes essaient d'extraire des données à caractère personnel de citoyens européens pour leur demander une rançon. Leur but est aussi de mettre à nu le système de protection de données de l'Europe et de montrer comment ses sociétés sont vulnérables. Les enquêteurs ont toutefois beaucoup de mal à prouver que ces attaques ont le soutien du Kremlin. Les quelques indices dont ils disposent ne sont pas suffisants, la plupart du temps, pour réclamer des explications à la Russie.



La réaction de Bruxelles

La Commission européenne et les États membres ont parfaitement compris qu'ils sont devenus la cible d'attaques cybernétiques. Ils constatent aussi que des failles de sécurité permettent à Moscou de continuer à opérer en toute impunité sur les réseaux européens.

Pour y remédier, la Commission européenne a mis à jour sa stratégie de cybersécurité en décembre 2020 et a proposé une nouvelle directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'Union (directive SRI 2). Ces deux initiatives visent à renforcer la capacité opérationnelle de l'UE pour lutter contre les cyberattaques, à étendre le réseau de protection à de nouveaux secteurs et à promouvoir l'investissement dans la cybersécurité des organisations européennes (inférieur de 41 % à celui des États-Unis).

De surcroît, l'Union européenne est encore plus aux aguets en raison du conflit entre la Russie et l'Ukraine au cours des dernières semaines. La Banque centrale européenne a demandé aux banques nationales de se préparer à repousser des attaques cybernétiques russes, tandis que la présidence française du Conseil de l'UE a lancé un simulacre de cyberattaque à grande échelle contre les chaînes logistiques des États membres.

Tout cela mène à une même conclusion : la guerre cybernétique a dépassé le cadre de la science-fiction. Elle a même véritablement débuté. Et bien qu'elle se déroule sans effusion de sang, elle a un effet direct sur la vie des citoyens. Face aux principales menaces que sont la Russie et la transformation numérique, l'Union européenne fourbit ses armes technologiques pour mettre tout le monde d'accord et faire du cyberespace un environnement sécurisé.

3. Déséquilibres de pouvoir et liberté de consentement : La forteresse numérique qu'est l'Europe

L'écosystème des données européennes de contrôle et de surveillance biométriques

Résumé : Une description des principaux systèmes utilisés en Europe pour gérer la mobilité des personnes à travers les frontières européennes et entre ses pays, avec un accent sur les aspects qui peuvent être améliorés des mécanismes actuels.

Auteur : Institut méditerranéen pour le reportage d'investigation (MIIR)

Lien : Disponible à partir du 26 avril 2022

Texte :

La numérisation et la mise en ligne d'un nombre croissant d'aspects de notre vie est une tendance à long terme accélérée par la pandémie de COVID-19. Cependant, ce qui passe largement inaperçu, c'est la même tendance impliquant les superpuissances de collecte de données et de surveillance des États de l'UE.

Les autorités nationales des États membres, telles que la police, les services de sécurité intérieure, les gardes-frontières, les services d'immigration et les organismes européens tels qu'Europol et Frontex, exploitent des infrastructures de collecte et de stockage de données à grande échelle. Sous couvert de "sécurité nationale", un espace est créé pour des violations potentielles des droits humains fondamentaux, à un moment où la sécurité "militarisée" aux frontières a déjà conduit à des violences contre les réfugiés, à des refoulements avec le risque de voir des personnes retourner dans des pays peu sûrs et dans des conditions inhumaines, et à une augmentation alarmante des décès évitables.

Les pays ferment les routes migratoires - à l'exception récente et discriminatoire des réfugiés ukrainiens - obligeant ainsi les migrants et les réfugiés à chercher d'autres solutions, souvent plus dangereuses, et les poussant dans les bras des réseaux criminels de passeurs.

Mais les murs physiques ne sont pas les seuls à être érigés ; comme le rapporte l'institut indépendant Transnational Institute TNI (Border War Series reports), une partie essentielle de la soi-disant "forteresse Europe" consiste en des "murs virtuels" qui visent à empêcher les migrants d'entrer dans l'espace Schengen ou à surveiller leurs mouvements à l'intérieur de celui-ci. Ces "murs virtuels" se présentent sous de nombreuses formes : des systèmes de surveillance avancés qui contrôlent les flux migratoires et suivent les mouvements des personnes aux frontières extérieures (et parfois avant) aux bases de données d'IA "intelligentes" et interopérables qui visent à identifier, enregistrer et profiler les migrants aux frontières et à l'intérieur de celles-ci.

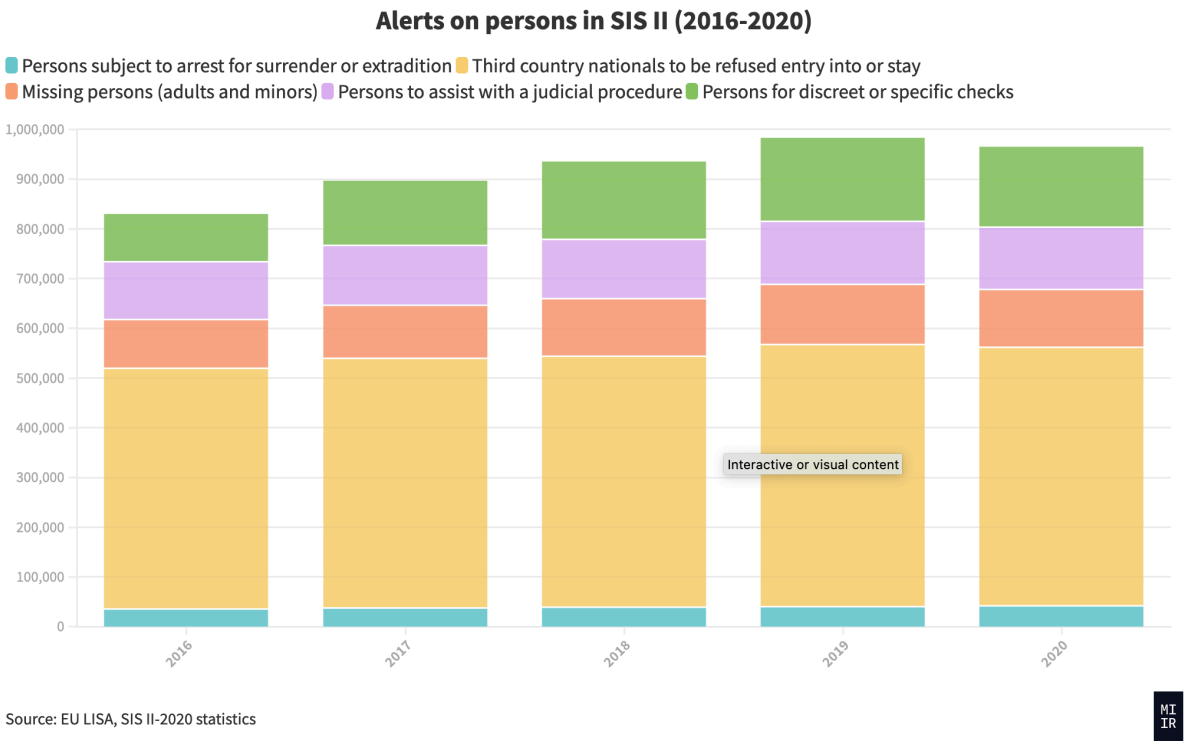
Le dénominateur commun des murs physiques et virtuels est la construction sociale même de "l'homme en mouvement" comme une menace potentielle pour l'UE et ses États membres. Les personnes qui tentent d'atteindre et d'entrer dans l'UE, fuyant les catastrophes, la violence, la guerre ou les persécutions politiques, sont considérées comme des facteurs de risque qui doivent être évalués et catégorisés.

L'équipe journalistique du MIIR dans le cadre du projet Panelfit (Participatory Approaches to a New Ethical and Legal Framework for ICT) a entrepris de pénétrer dans les différents systèmes d'enregistrement et de surveillance des données de l'UE, d'étudier leur législation et les données collectées dans les différentes bases de données, afin d'identifier les risques pour les droits de l'Homme également créés par l'interopérabilité de ces systèmes, sur la base de nombreux entretiens avec des experts dans le domaine, des chercheurs, des activistes, des avocats, des ONG et des migrants. Dans la première partie de la recherche, nous présentons un bref aperçu des principaux systèmes de surveillance.

Description des systèmes d'enregistrement et des bases de données à caractère personnel

1. SIS-II Système d'information Schengen

La base de données la plus ancienne. Elle a pour but de contrôler les mouvements des ressortissants de pays tiers dans les espaces Schengen. Elle a été créée en 1995 pour être mise à jour dans sa deuxième version en 2013 et à partir des mois suivants, les dispositions incorporées en 2018 entreront en vigueur. Il s'agit du plus grand système informatique d'Europe, qui fonctionne dans 26 États membres de l'UE (Chypre n'est pas inclus mais devrait y adhérer) ainsi qu'en Suisse, en Norvège, au Liechtenstein et en Islande. En vertu du règlement SIS II, les données (noms, prénoms, dates de naissance et autres informations alphanumériques) des ressortissants de pays tiers faisant l'objet d'une décision de retour, les données relatives au refus d'entrée ou de séjour de personnes dans l'espace Schengen, ainsi que des objets (par exemple, des voitures, des armes, des documents perdus, des passeports, etc.) sont collectés et traités aux fins de la coopération policière et judiciaire. Les dispositions du règlement SIS II permettent l'identification biométrique des personnes basée sur la technologie de reconnaissance faciale. Elle est utilisée tant par les autorités de police que par les autorités chargées de l'immigration et de l'asile. Si une personne demande l'asile, les autorités peuvent effectuer une recherche dans le SIS pour voir s'il existe un signalement la concernant. Les signalements peuvent concerner des personnes recherchées pour arrestation ou contrôle, des personnes surveillées par les services répressifs, des personnes qui n'ont pas le droit d'entrer ou de séjourner dans l'UE, des personnes recherchées pour assistance judiciaire et des personnes disparues (adultes et enfants).



En 2019, le système SIS II a établi un record avec 18 millions de recherches par jour par toutes les autorités compétentes habilitées à y accéder. Ce chiffre est d'ailleurs trois fois supérieur au nombre de recherches effectuées en 2014 (6 millions de recherches par jour). L'introduction, fin 2020, de l'application AFIS (Automated Fingerprint Identification System), permettant des recherches par États et par empreintes digitales et introduisant une vérification et une comparaison automatiques avec les recherches existantes, est révélatrice de cette utilisation généralisée.

Toutefois, un indice de l'utilisation élargie ciblée du système pour identifier les sans-papiers est que sur les 964 720 signalements effectués dans le SIS II en 2020, plus de la moitié concernaient des ressortissants de pays tiers qui s'étaient vu refuser l'entrée et le séjour dans l'espace Schengen. Cela a été le cas de manière constante au fil des ans, comme le montre le tableau des signalements 2016-2020.

2. VIS - Système d'information sur les visas

Il a été progressivement mis en place à partir de 2011 et le développement du système s'est achevé en 2016. Le système est utilisé par les 30 États Schengen ainsi que par la Bulgarie, la Croatie, Chypre et la Roumanie. L'objectif est de permettre à ces pays d'échanger des données sur les visas de court séjour et de faciliter le contrôle des visas aux postes frontières. Les autorités compétentes en matière d'asile peuvent accéder au VIS. En 2018, la Commission européenne a présenté une proposition de révision du VIS afin d'en élargir le champ d'application. Les règles proposées suggèrent que le VIS devrait également inclure des données sur les visas de long séjour.

VIS: Use of biometrics, searches and access

68 million facial images stored in the VIS
By the end of 2019

69 million fingerprints sets stored
By the end of 2019

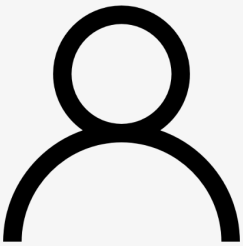
100 million records capacity
By the end of 2019

7 million biometric searches in 2019 (2018: 8 million)
Searches in 2019

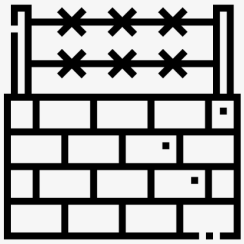
17 million biometric authentications in 2019 (2018: unchanged)
Searches in 2019

25 million alphanumeric searches in 2019 (2018: 23 million)
Searches in 2019

116 national authorities granted access
Access



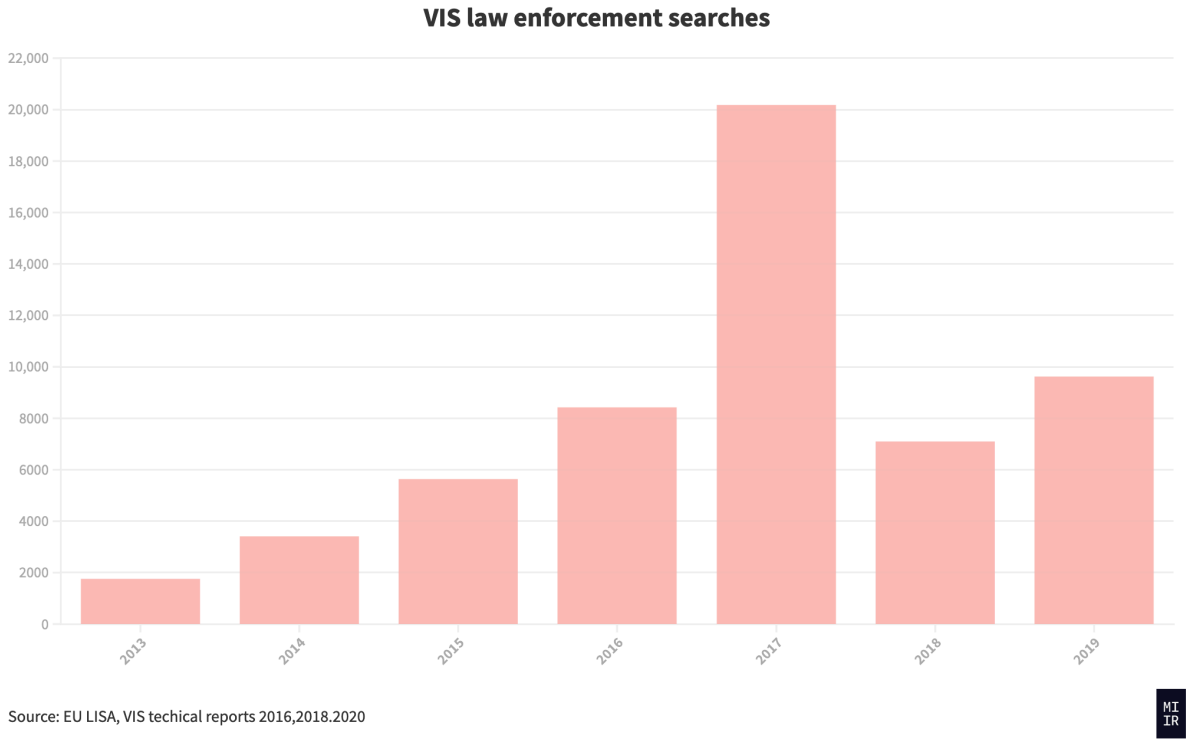
458.000, total number of end-users accessing VIS
Access



84 million border checks (visa verification and identification)
Border checks

Le système stocke les empreintes digitales et une photographie des demandeurs/titulaires de visa, ainsi que les données personnelles incluses dans leurs demandes, telles que le nom de famille, l'adresse du domicile, les informations sur le statut du visa et les données bancaires (preuve de dépôt). "Sans ces données, le visa ne sera pas accordé. Il s'agit implicitement d'une discrimination de classe : si vous êtes riche, vous pouvez voyager, si vous n'avez pas d'argent, ils ne vous accorderont raisonnablement pas de visa ("low-tech discrimination"). Le montant dépend de chaque État membre", explique le chercheur Georgios Glouftios.

L'identification biométrique automatisée est déjà utilisée dans le VIS sur la base des empreintes digitales collectées. En 2019, 7 millions de recherches biométriques ont été effectuées et 17 millions de contrôles d'identité biométriques ont été réalisés, ces derniers principalement aux postes frontières. Dans les aéroports, les autorités contrôlent les ressortissants de pays tiers qui se rendent en Europe pour s'assurer que leurs empreintes digitales correspondent à celles de leur dossier individuel dans le système VIS, qui est obligatoirement mis en place avant le voyage. Les autorités de police peuvent effectuer des recherches dans le VIS afin de déterminer si une personne qui a déjà demandé un visa est impliquée dans une activité criminelle. Il peut également être utilisé par les autorités compétentes en matière d'asile.



Un autre élément qui exacerbe les préoccupations des citoyens et des organisations en matière de respect de la vie privée à l'égard de ces systèmes est l'accès étendu des agences et des personnes de tous les services. Il est peut-être vrai que, chaque année, les autorités de chaque pays qui ont le droit d'accéder à la base de données sont publiées dans le Journal de l'UE. Mais cela ne suffit pas, car le nombre d'utilisateurs finaux susceptibles d'avoir accès aux données personnelles des personnes est incertain. Par exemple, dans le système VIS, un total de 116 services et autorités nationales, y compris

les services répressifs, sont autorisés à créer, modifier et supprimer des données - et le nombre d'utilisateurs finaux atteint le chiffre astronomique de 458 000 employés, qui ont tous accès à ces données personnelles sensibles.

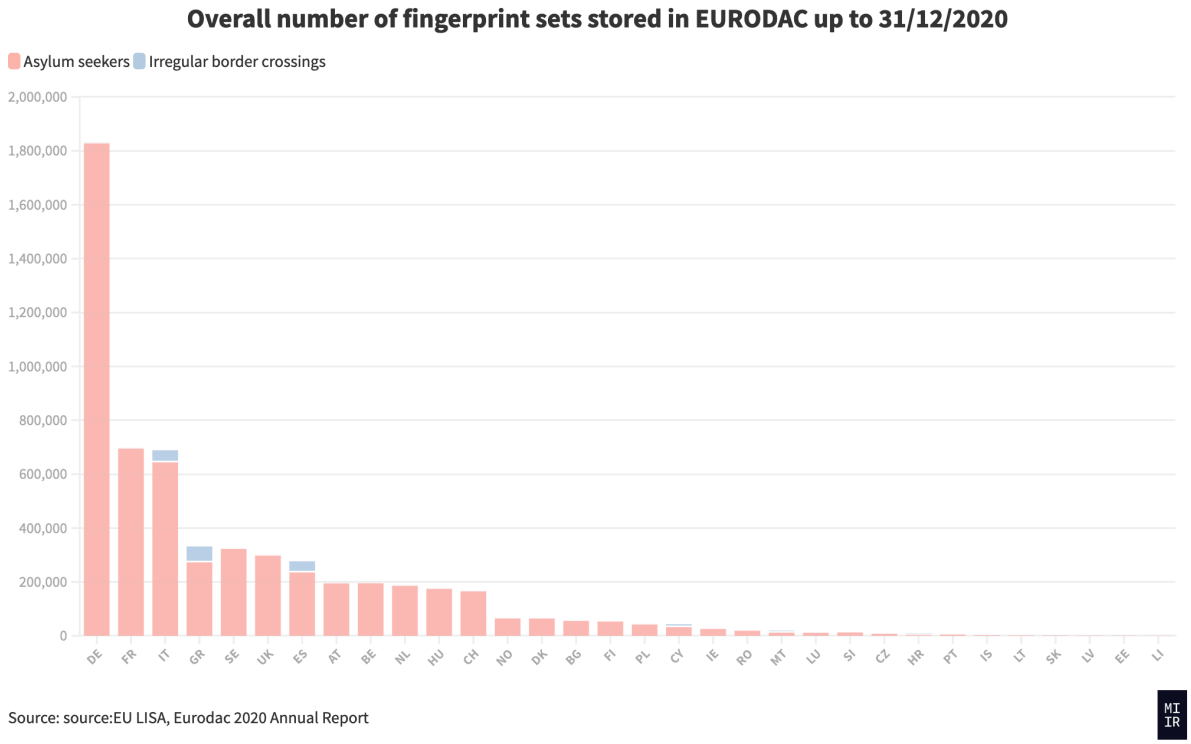
3.Eurodac

Le système européen de comparaison des empreintes digitales des demandeurs d'asile (EURODAC) est devenu opérationnel en 2003, en tant que premier système informatique permettant le stockage des empreintes digitales dans une base de données au niveau de l'UE. L'objectif du système était de permettre aux pays de l'UE de déterminer plus facilement la responsabilité de l'examen d'une demande d'asile en comparant les empreintes digitales des demandeurs d'asile et des ressortissants de pays tiers/non EEE avec une base de données centrale. En outre, l'objectif était de permettre aux services répressifs, dans des conditions strictes, d'effectuer des recherches dans Eurodac à des fins d'enquête, de détection et de prévention des infractions terroristes ou des infractions pénales graves. Jusqu'à présent, Eurodac ne stocke que les caractéristiques biométriques, et n'enregistre même pas le nom d'une personne. Lorsqu'un demandeur d'asile ou un ressortissant d'un pays tiers/non-EEE est trouvé en situation irrégulière dans un pays de l'UE, ce dernier peut consulter Eurodac pour savoir si la personne a déjà demandé l'asile dans un pays de l'UE ou a déjà été arrêtée alors qu'elle tentait d'entrer illégalement dans l'UE.

EURODAC est actuellement en cours de révision. Les révisions proposées prévoient l'interaction d'EURODAC avec d'autres systèmes informatiques de l'UE dans le cadre des procédures d'asile, de retour et de réinstallation. Dans ce contexte, EURODAC sera utilisé, entre autres, pour le contrôle des flux migratoires et la détection des mouvements secondaires de ressortissants de pays tiers en situation irrégulière.

Toutefois, les chiffres montrent que la collecte et le stockage des empreintes digitales de ressortissants de pays tiers ou d'apatrides sont également une pratique courante. En particulier, les États membres ont transmis un total de 644 926 ensembles d'empreintes digitales à EURODAC en 2020. Parmi ceux-ci, 62% représentent des ensembles d'empreintes digitales de demandeurs de protection internationale, 25% représentent les empreintes digitales de ressortissants de pays tiers ou d’apatrides trouvés en séjour illégal dans un État membre, tandis que 13% sont celles des mêmes groupes trouvés en train de franchir illégalement la frontière extérieure.

La nouvelle proposition, si elle est adoptée, rendra obligatoire la collecte et le stockage des empreintes digitales des ressortissants de pays tiers ou des apatrides en séjour irrégulier en Europe. En outre, le volume des données personnelles collectées sera radicalement augmenté. Les dispositions proposées permettront la collecte d'une grande variété d'informations biographiques et biométriques en plus de celles déjà collectées, telles que les images des personnes, les noms, la date et le lieu de naissance, et la nationalité.



Les près de 6 millions d'empreintes digitales accumulées dans EURODAC à la fin de 2020 n'appartiennent pas exclusivement à des demandeurs d'asile, mais aussi à des migrants que les États d'accueil ont classés comme "franchisseurs irréguliers de frontières", qui n'ont pas le droit d'accéder aux procédures d'asile. Au 31/12/2020, date de l'enregistrement, ils n'étaient que près de 155 000 (3%), mais les empreintes digitales de cette catégorie sont automatiquement effacées de la base de données après 18 mois, contrairement à celles des demandeurs d'asile, qui sont conservées pendant 10 ans. Ainsi, la proportion correspondante pour ces derniers à la fin de 2016 était de 13%. Il faut noter que depuis juillet 2015, la base de données EURODAC est également accessible aux services de police des pays et à Europol au nom de la prévention et de l'investigation des infractions liées au terrorisme et à la grande criminalité.

Il est intéressant de noter que l'Allemagne, bien que n'étant pas un pays de premier accueil comme l'Italie et la Grèce, semble néanmoins accumuler la grande majorité des données biométriques parmi les 32 pays Segen. Cela s'explique par le fait qu'une grande majorité des migrants qui sont arrivés en Europe notamment avec la crise des réfugiés de 2015 ont demandé l'asile pour la première fois en Allemagne, et non dans les pays situés aux points d'entrée des frontières européennes. Dans le classement du stockage biométrique, les pays qui suivent l'Allemagne sont la France, l'Italie, la Grèce, la Serbie, le Royaume-Uni et l'Espagne.

Il est également frappant de constater que la Grèce est le "leader" parmi les 32 pays dans la collecte des empreintes digitales des migrants qui n'ont pas droit à l'accès à l'asile. Cela représente 56 000 (c'est-à-dire un tiers du total de cette catégorie dans EURODAC) sur un total de 331 609 empreintes

digitales enregistrées par la Grèce à la fin de 2020. La remarquable première place de la Grèce est liée au processus d'enregistrement des données et de dépistage dans les centres d'accueil grecs pour les migrants entrant dans le pays.

La première étape officielle de l'enregistrement, en plus de la vérification des documents pertinents que la personne peut porter sur elle (passeport, carte d'identité, autres documents) est l'examen/interview/interrogatoire par la police grecque ou le personnel de FRONTEX, ce qu'on appelle le screening. "L'objectif de cette procédure est de "calibrer" l'identité de la personne, c'est-à-dire des données telles que l'âge, la nationalité, le lieu d'origine, les relations familiales, et elle est effectuée en coopération avec les traducteurs de FRONTEX", explique Vassilis Vlassis, chercheur post-doctoral sur les technologies de surveillance à l'Université d'informatique de Copenhague. Il a mené une étude de terrain sur les procédures d'asile et de dépistage dans les centres d'accueil de Chios et Lesvos. "Il ressort des entretiens que j'ai menés avec des personnes qui étaient chargées du filtrage à VIAL, à Chios, que de nombreuses données sont examinées : la parole, la prononciation, l'orthographe, les vêtements, les bijoux et, bien sûr, les photos des téléphones portables, etc. sont tous examinés et pris en compte dans la conclusion que tirera l'agent de filtrage : "Je sais que les Syriens épellent Mohamad comme ceci et jamais comme cela, tandis que les Marocains l'épellent comme ceci, mais jamais comme cela", m'a-t-on dit. L'instinct, l'intuition jouent aussi leur rôle. Parfois, dès qu'ils franchissent la porte, vous avez immédiatement une opinion, puis vous cherchez à la valider, comme l'a également dit l'un des auditeurs", raconte Vlasis. En conclusion, la manière dont ces données prennent forme est multifactorielle et comporte de forts éléments performatifs, mais elle peut néanmoins avoir un impact décisif sur l'avenir du migrant qui rejoint EURODAC. "Le coordinateur de la mission FRONTEX dans les îles grecques en 2016 m'a lui-même dit : "le résultat du dépistage ne constitue pas un fait scientifique. C'est une hypothèse de travail, le mieux que nous puissions faire et ce avec quoi nous travaillons", raconte Vlassis.

4. EES (système européen d'entrée/sortie)

Créé en 2017, il devrait être pleinement opérationnel en mai 2022. Il recueille des données sur tous les ressortissants de pays tiers, qu'ils aient besoin de demander un visa ou non. Il enregistre et stocke la date, l'heure et le lieu d'entrée et de sortie des titulaires d'un visa de court séjour et des voyageurs exemptés de l'obligation de visa lorsqu'ils franchissent la frontière de l'UE. Le système vise à remplacer la procédure du tampon de passeport en permettant le traitement des données biométriques des personnes. Il permet également d'enregistrer la durée du séjour d'une personne et de créer des alertes automatiques en cas de "dépassement de la durée de séjour" dans un pays. Les autorités répressives nationales et Europol pourront accéder à cette base de données.

5. ETIAS - (Système européen d'information et d'autorisation concernant les voyages)

Créé en 2018, l'objectif est d'être pleinement opérationnel d'ici décembre 2022. Selon les déclarations de l'UE, il s'agit d'"un système informatique largement automatisé qui sera mis en place pour identifier les risques en matière de sécurité, de migration irrégulière ou de forte épidémie que

présentent les visiteurs se rendant dans les États Schengen et qui ne sont pas soumis à l'obligation de visa. [...] Les ressortissants de pays tiers qui n'ont pas besoin d'un visa pour se rendre dans l'espace Schengen doivent demander une autorisation de voyage par le biais du système ETIAS avant de voyager." C'est un nouvel exemple de l'UE qui traite les personnes qui prévoient de se rendre en Europe comme des facteurs de risque. Le système ne stockera aucun type d'informations biométriques. Toutefois, différentes catégories de données seront collectées, telles que le nom de famille du demandeur, sa nationalité, son pays et sa ville de résidence, son adresse personnelle, son adresse électronique et son numéro de téléphone, son niveau d'instruction (primaire, secondaire, supérieur ou sans instruction).

En pratique, le système ETIAS fonctionnera à peu près de la même manière que le système ESTA aux États-Unis.

6. ECRIS-TCN (Système européen d'information sur les casiers judiciaires qui concerne les ressortissants de pays tiers)

Créé à l'origine en 2012, ECRIS permet l'échange efficace d'informations entre les États membres concernant les condamnations pénales dans l'UE. La plupart des informations échangées concernent des citoyens européens. Le système européen révisé d'information sur les casiers judiciaires comprendra désormais une base de données centrale d'informations sur les condamnations des ressortissants de pays tiers et des apatrides (ECRIS-TCN) et devrait être opérationnel en 2022. Les données biographiques et biométriques des ressortissants de pays tiers, des apatrides et des citoyens de l'UE qui sont des ressortissants de pays tiers et ont été condamnés dans un État membre sont stockées dans l'ECRIS-TCN. Ces données comprennent des catégories telles que les noms et prénoms, le lieu et la date de naissance, la nationalité, le sexe, les numéros d'identité, ainsi que les données relatives aux empreintes digitales recueillies conformément à la législation de l'État membre au cours de la procédure pénale. Les images faciales des personnes condamnées seront également stockées dans le système si la législation de l'État membre de condamnation autorise la collecte et le stockage des images faciales des personnes condamnées. La base de données sera disponible sur Internet et les autorités pourront facilement y effectuer des recherches grâce à un mécanisme de recherche positive/négative : un résultat de recherche positif permettra d'identifier les États membres auprès desquels des informations complètes sur le casier judiciaire d'une personne donnée peuvent être obtenues.

L'ECRIS a été utilisé environ 3 millions de fois par an pour échanger des informations sur des condamnations pénales antérieures. Environ 30% des cas dans lesquels des informations sur les casiers judiciaires sont demandées reçoivent une réponse positive.

Selon la Commission Meijers, un groupe de professeurs de droit, de chercheurs, de juges et d'avocats qui veille à ce que la législation européenne respecte l'État de droit et garantisse les droits fondamentaux pour tous, le règlement ECRIS-TCN est la première législation européenne à traiter comme des ressortissants de pays tiers les citoyens européens qui sont également des ressortissants d'un pays tiers.

Interopérabilité des systèmes

Les serveurs de tous ces systèmes sont situés à Strasbourg. Ils y sont gérés par le service EU-Lisa. Lorsque nous pensons aux contrôles aux frontières et aux contrôles de mobilité, nous pensons généralement à Frontex, mais Frontex n'est pas le principal acteur de ces bases de données. EU-Lisa, l'Agence européenne pour la gestion opérationnelle des systèmes à grande échelle dans l'espace de liberté, de sécurité et de justice, fonctionne depuis 2012, est basée à Tallinn, en Estonie, mais son centre opérationnel est à Strasbourg. Elle a coordonné l'expérimentation du projet pilote "Frontières intelligentes" et les actions qui en découlent, l'analyse des résultats et l'établissement de rapports sur ce projet, en étroite collaboration avec les pays de l'UE participants et les institutions européennes. EU-Lisa est responsable de la gestion opérationnelle d'EURODAC, du SIS II, du VIS et d'Entry-ExitSystem, tout en assurant la sécurité des informations et la protection des données.

En 2019, l'UE a adopté deux règlements mettant en place un cadre juridique exigeant l'interopérabilité de 6 des bases de données décrites ci-dessus (VIS, SIS II, Eurodac, système d'entrée-sortie, ECRIS-TCN et ETIAS). L'objectif est de mettre en œuvre le système général d'interconnexion des données d'ici à la fin de 2023.

Si la Commission européenne présente l'interopérabilité comme une progression naturelle, dans la pratique, ce n'est pas le cas, car de nombreuses bases de données existantes ne sont pas encore totalement opérationnelles.

"Point de non-retour"

Selon le Contrôleur européen de la protection des données, la décision du législateur européen de rendre ces systèmes interopérables signifierait un "point de non-retour", avec de profondes implications pour le droit à la vie privée des personnes entrant dans l'UE. Une nouvelle base de données centrale contenant des informations sur des millions de ressortissants de pays tiers, y compris leurs données biométriques, aurait un accès nouveau et amélioré aux systèmes d'information.

Quatre autres plateformes de collecte de données dans l'UE deviendront opérationnelles ou devraient étendre leur champ d'action au cours des deux prochaines années. Le portail de recherche européen (ESP) permettra aux autorités compétentes nationales et européennes, lorsqu'elles ne sont pas en mesure d'identifier une personne ou qu'elles ont des doutes sur l'identité fournie, de lancer une requête en soumettant des données biographiques ou biométriques à l'ESP, qui effectuera une recherche

simultanée dans les six bases de données. Le service de correspondance biométrique créera et stockera des modèles à partir de toutes les données biométriques enregistrées dans les systèmes sous-jacents. Le Common ID Repository (CIR) stockera un enregistrement individuel pour chaque personne inscrite dans les systèmes, qui contiendra des données biométriques et biographiques. Enfin, le détecteur d'identités multiples sera en mesure de vérifier par recoupement les identités dans tous les systèmes.

Comme l'indique le rapport Technological Testing Grounds du réseau EDRI et du Refugee Law Lab, rédigé par Petra Molnar, ce cadre d'interopérabilité unique fournit une infrastructure favorable à de nombreux processus décisionnels automatisés qui mettent en danger les droits de l'Homme. Chris Jones, directeur de Statewatch, auteur du rapport "Automated suspicion : the EU's new travel surveillance initiatives", a déclaré : "L'enthousiasme des fonctionnaires de l'UE et des États membres pour l'utilisation de nouvelles techniques et de nouveaux outils sur des voyageurs peu méfiants est inquiétant, car ils augmentent le risque de discrimination, peuvent conduire à de nouvelles erreurs dans la prise de décision et transmettront davantage de données personnelles aux gouvernements. Les gens devraient réfléchir davantage à la manière dont leurs gouvernements traitent les étrangers - sinon ils risquent eux aussi d'être traités comme des suspects plutôt que comme des citoyens."

Il convient également de noter l'absence totale d'évaluation par le législateur de l'impact des nouveaux systèmes interopérables sur les droits de l'Homme, ainsi que des ressources et de la portée des autorités indépendantes qui contrôlent ces systèmes, afin de leur demander des comptes.

L'un des pièges du développement technologique est que nous avons tendance à croire qu'il va accroître l'efficacité et aider à atteindre les objectifs pour lesquels il a été conçu. Trop souvent, ce n'est pas le cas. Un premier problème majeur qui se pose a trait à la qualité des données saisies dans certaines des bases de données susmentionnées que nous avons présentées. "Par exemple, selon un rapport récemment publié par la Cour des comptes européenne, il existe un problème majeur de qualité des données introduites dans le système d'information Schengen. Et par qualité, on entend aussi bien les données biométriques que les données alphanumériques. Il peut arriver, par exemple, qu'un policier d'un État membre orthographie mal le nom d'une personne recherchée lorsqu'il introduit un signalement dans le système ou qu'il saisisse le nom d'une personne dans le champ de données consacré aux noms de famille", explique le chercheur Georgios Glouftios. Si une personne est enregistrée dans une base de données avec un nom incorrect ou d'autres données de mauvaise qualité, deux problèmes peuvent survenir. Le premier concerne les faux négatifs : les personnes recherchées ou suspectées ne sont pas identifiées par le système simplement parce que leur nom n'est pas correctement enregistré dans la base de données. L'autre problème concerne les faux positifs, c'est-à-dire l'identification incorrecte d'une personne. Par exemple, une personne est contrôlée par la police pour une raison quelconque et, par erreur, son nom est très similaire ou identique à celui d'un mauvais

signalement stocké dans un système. Dans ce cas, elle peut avoir des ennuis, précisément parce que le système l'a identifiée à tort comme une personne recherchée.

"Je pense qu'il y a trois problèmes principaux en termes de précision des technologies appliquées pour la sécurité des frontières. Premièrement, la mauvaise qualité des données. Deuxièmement, le manque d'exhaustivité des données. Et troisièmement, et cela concerne davantage les développements futurs, des données biaisées et des décisions de sécurité potentiellement biaisées", déclare Georgios Glouftios.

* Citation tirée de l'ouvrage "Technological Testing Grounds, Migration Management Experiments and Reflections from the Ground Up" (EDRi, laboratoire de droit des réfugiés, novembre 2020, auteur Petra Molnar).

Piégé dans un système de surveillance numérique

Résumé : L'impact des systèmes de surveillance sur les populations vulnérables, l'argent pour les drones de Frontex, et le contrôle de la circulation des citoyens dans l'espace européen.

Auteur : Kostas Zafeiropoulos, Ioanna Louloudi, Nikos Morfonios (MIIR)

Lien : Disponible à partir du 26 avril 2022

Texte :

Au consulat de Grèce à Istanbul, un matin de 2016, Erkan, un citoyen turc d'origine kurde, franchit le seuil du bâtiment pour s'adresser aux autorités grecques. Il cherche à obtenir un visa pour entrer en Grèce afin de fuir la Turquie à un moment où le régime d'Erdogan multiplie les persécutions, notamment contre les dirigeants et les membres du parti d'opposition HDP et ses partisans kurdes. L'autorité consulaire grecque a toutefois rejeté la demande de visa et Erkan a été contraint de rester en Turquie.

Orestiada Evros, 4 ans plus tard. Erkan a été arrêté à la frontière gréco-turque alors qu'il tentait de pénétrer sur le territoire grec et a été traduit en justice. Le tribunal l'a condamné à 4 ans de prison sans sursis et à une amende de 10 000 euros pour être entré à nouveau dans le pays. Mais Erkan n'était pas rentré en Grèce.

Que s'était-il passé ? Devant des juges grecs, Erkan a demandé l'asile à la Grèce pour persécution par le régime d'Erdogan, mais on lui a dit que son nom figurait sur la liste nationale des étrangers indésirables (EKANA) et sur le système d'information Schengen (SIS II, le plus grand système d'échange d'informations entre les pays de l'espace Schengen), avec une note indiquant qu'il était interdit d'entrée dans le pays depuis 7 ans. En raison de son inscription sur ces listes, il a été emmené d'abord à la prison de Komotini, puis à celle de Corfou.

"Nous essayions de savoir ce qui s'était réellement passé", raconte l'avocate d'Erkan et de Human Rights 360, Eugenia Kouniaki. "Mon client n'était jamais entré en Grèce auparavant et il a soudainement été condamné pour être rentré dans le pays. Dans un premier temps, j'ai contacté les autorités policières, le directeur du service d'asile à Athènes, où il m'a répondu que mon client avait été inclus dans l'EKANA et le SIS II parce que son visa avait été rejeté par le consulat à Istanbul."

La vérité se trouvait tout simplement dans le fonctionnement du système européen unique d'information sur les visas (VISA-VIS) et du SIS II. Le consulat grec qui a traité la demande d'Erkan a inscrit le refus de visa dans le système VIS et dans le SIS II en même temps. À partir de ce moment-là, cet enregistrement a suffi à le mettre sur la voie de la prison, même s'il demandait une protection internationale.

"Même lorsque j'ai demandé son retrait de la liste des indésirables et du SIS II, car Erkan était un demandeur d'asile, la police grecque a refusé", décrit Kouniaki. "Outre le fait que mon client ne savait pas qu'il était sur la liste, lorsque nous avons essayé de savoir pourquoi son visa avait été refusé en 2016, nous avons reçu la vague réponse "pour avoir falsifié certains documents"". Lorsque nous avons tenté de savoir quels documents étaient prétendument falsifiés, nous n'avons pas pu vérifier de quoi il s'agissait. Heureusement, lors du recours que nous avons déposé pour obtenir un délai d'exécution de la peine, les juges ont accepté nos arguments et, au bout d'un an, il a été libéré de prison."

Cependant, après tout ce traitement injuste et cet emprisonnement, il a préféré quitter le pays "parce qu'il croyait qu'il ne trouverait jamais justice", conclut Kouniaki.

Se brûler les doigts pour éviter l'identification dans EURODAC

L'histoire d'Erkan peut paraître scandaleuse, mais elle n'est malheureusement pas la seule liée aux conséquences des technologies de surveillance et des systèmes de données biométriques pour les migrants. Dans le rapport "Technological Testing Grounds : migration management experiments and reflections from the ground up" (EDRi, Refugee Law Lab, novembre 2020), l'auteur Petra Molnar, avocate et membre d'EDRi (European Digital Rights), a recueilli une multitude d'entretiens avec des demandeurs d'asile à Bruxelles qui sont entrés en contact avec des systèmes de contrôle de la mobilité pendant leur voyage vers la sécurité en Europe.

Caleb, un homme marié d'une trentaine d'années, décrit son expérience de la procédure d'asile en disant qu'il s'est senti "comme un morceau de viande sans vie, juste des empreintes digitales et des scans d'iris". Un autre migrant, Esche, décrit sa rencontre avec les drones en Méditerranée et dans la Manche avec une citation dévastatrice au moment où elle les a vus dans le ciel : "maintenant nous avons des ordinateurs volants au lieu de plus d'asile".

L'histoire la plus désagréable est racontée par Negassi, un jeune homme de 20 ans originaire d'Éthiopie : "Je suis fatigué et je veux aller en Angleterre", dit-il après avoir été bloqué à Bruxelles pendant près de deux ans, sans papiers, et avant cela à Nuremberg pendant cinq ans. Mais ce n'est pas la première fois qu'il se retrouve en Belgique, puisqu'il a déjà été expulsé vers l'Allemagne après avoir été arrêté dans un parc de Bruxelles, où il dormait dans la rue. Lorsque ses données biométriques ont été relevées par la police belge, ses empreintes digitales ont donné un résultat positif dans le système EURODAC, qui stocke et identifie les empreintes digitales des demandeurs d'asile, l'identifiant comme un demandeur d'asile en Allemagne pour la première fois. Ils l'ont donc renvoyé en raison de Dublin II, qui stipule que le premier pays d'accueil doit traiter la demande.

Negassi reconnaît que le processus de collecte des données biométriques est invasif pour le corps, mais il s'interroge : "Comment puis-je refuser quand la police me menotte, m'emmène au poste et m'oblige à donner mes empreintes digitales ?" dit-il à Molnar. Il a des amis qui sont allés jusqu'à se brûler les doigts pour modifier leurs empreintes digitales et éviter l'identification. "Toutefois, cela ne résout pas le problème" pour Negassi, car l'absence d'identification signifie généralement une période de détention plus longue.

"Il y a un aspect très important qui n'est pas assez discuté dans le débat public, nous dit Petra Molnar, et qui concerne le fait que ces technologies de surveillance provoquent des traumatismes chez des personnes qui ne sont même pas familières avec la technologie. Les migrants à qui j'ai parlé avaient tous en eux la conviction profonde qu'ils subissaient un traitement raciste et discriminatoire au contact de ces systèmes."

C'est pourquoi il est encore plus important, poursuit-il, "face à l'utilisation effrénée de ces technologies, qu'il y ait une responsabilité, une surveillance et une gouvernance. Nous devons nous concentrer sur le type de structures de gouvernance à développer pour garantir que ces technologies, qui représentent un risque pour les droits de l'Homme, ne causent pas de traumatismes aux personnes."

La partie responsabilité, cependant, ne semble pas être renforcée par la manière dont ces systèmes sont développés. L'implication des entreprises privées dans les industries de la sécurité et de la défense complique encore les choses. "Il existe une relation très problématique entre les entreprises privées et les institutions publiques qui travaillent ensemble sous prétexte que les États eux-mêmes ne peuvent pas développer ces technologies en interne", souligne M. Molnar. "D'énormes ressources publiques sont donc dirigées vers les grandes entreprises pour les développer. Mais aussi d'un point de vue juridique, cela crée le problème de ce que certains appellent le "blanchiment de responsabilité" lorsque quelque chose tourne mal. Dans ces cas-là, comme nous l'avons vu, l'État dit "ce n'est pas notre problème car nous n'avons pas développé cette technologie". Et l'entreprise privée, de son côté, rétorque que "c'est la gestion étatique des outils qui est à blâmer"."

Mais les budgets publics consacrés au complexe industriel de la gestion des migrations et du contrôle des frontières sont considérables, souligne Molnar. "De tout cet argent dans une technologie aussi problématique qui inflige des traumatismes, imaginez s'il allait à l'éducation, aux services juridiques, au logement. Pourquoi les États, au lieu de déverser autant d'argent dans les technologies de surveillance, ne réfléchissent-ils pas à la manière de l'utiliser pour l'inclusion sociale ?"

Le système européen de surveillance des frontières (Eurosur) et l'argent pour les drones

Le système le plus intéressant pour les questions de migration est peut-être Eurosur, qui produit des cartes des frontières territoriales/terrestres et maritimes. Il est exploité par Frontex et permet l'échange de cartes entre les États concernant les contrôles aux frontières en mer. "Le développement d'Eurosur a été lancé en 2007, mais il parvient au Parlement européen pour la première fois fin 2012, après que des centaines de millions ont été dépensés et que sa conception a été achevée, mettant effectivement l'institution devant le fait accompli. En raison du manque de transparence, la recherche dans les directions concernées de la Commission européenne est largement captée par les priorités du complexe sécurité-industrie", rapporte le journaliste Apostolis Fotiadis dans son livre "Border Merchants".

Lors de sa conception, il a été présenté comme une "technologie humanitaire", un système qui permettrait aux autorités de chaque État membre de mener des opérations de recherche et de sauvetage. L'idée était que "nous utilisons des cartes, nous obtenons des informations à partir de satellites et aussi de drones, pour percevoir les flux migratoires, par exemple de l'Afrique vers l'Europe, afin de pouvoir sauver des personnes en mer". Le problème est qu'Eurosur crée des images dites "pré-frontières". Il s'agit de cartes qui se concentrent sur la zone avant la frontière, avant qu'un navire n'arrive à la frontière maritime, par exemple la Grèce. "Ils le font principalement pour organiser des opérations de repli, car par exemple les autorités italiennes peuvent partager des données avec les autorités libyennes pour que ces dernières puissent reprendre les migrants. Ils savent que les push-backs ne sont pas autorisés, la solution est donc le pull-back. C'est pourquoi la Libye est financée", explique au MIIR Georgios Glouftios, professeur à l'université de Trente.

Pour la création des cartes pré-frontières, Frontex coopère également avec le Centre satellitaire de l'Union européenne (EU SatCen), qui lui fournit des images satellites, des photographies aériennes et d'autres services connexes. La base de données Eurosur enregistre également les incidents survenus aux frontières maritimes de l'UE, bien que les États membres n'aient pas été obligés jusqu'à présent de télécharger les données relatives aux incidents survenus aux points de contrôle frontaliers de manière systématique et organisée (cela a changé avec un règlement d'application en avril 2021). Cela signifie qu'il n'existe pas d'enregistrement complet et méthodique des incidents, ce qui brouille l'image globale des incidents aux frontières extérieures. Un fait qui est également admis par la Commission européenne dans le rapport d'évaluation d'Eurosur (septembre 2018).

Le deuxième rapport de Frontex en 2018 sur le fonctionnement d'Eurosur a recensé plus de 184 000 incidents sur la période allant de décembre 2013 à début 2018, la grande majorité (147 827) étant liée aux flux migratoires.

Events inserted in Eurosur 2013-2018

Eurosur Node	Crisis	Irregular migration	Related crossborder crime	Other	Total events
Member State	66	83,845	20,641	686	105,238
Frontex	80	63,982	12,231	3029	79,322
Total	146	147,827	32,872	3715	184,560

Source: Frontex

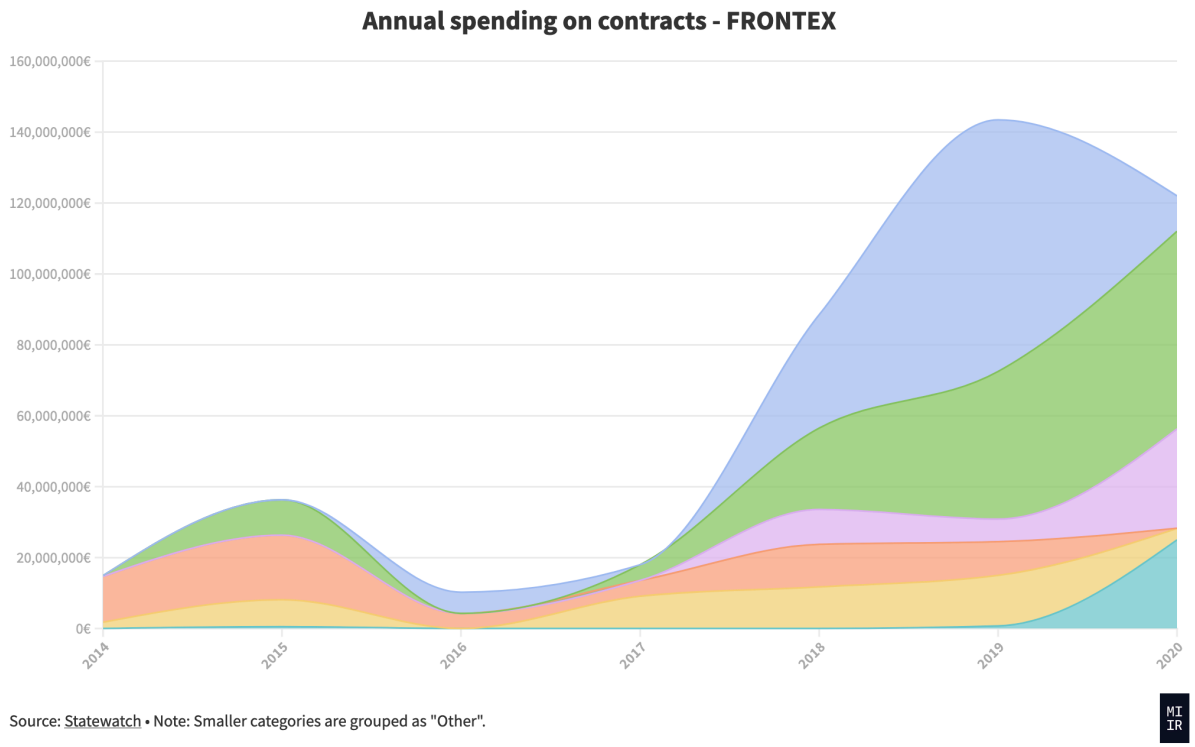
En février 2022, le gouvernement français a annoncé qu'il allait installer des caméras supplémentaires le long des côtes de la Manche afin de surveiller les migrants qui espèrent traverser la Manche pour rejoindre le Royaume-Uni. Les caméras sont payées par le gouvernement britannique. En décembre 2021, la marine italienne a livré une nouvelle cargaison de conteneurs contenant des équipements de surveillance à la Libye pour surveiller les migrations en Méditerranée (source : magazine de recherche Altreconomia, numéro de février 2021). Des "caméras-pièges" supplémentaires pour les voitures et les personnes ont également été placées à la frontière entre l'Italie et la Slovénie ou à proximité, le long de la "route des Balkans".

Les yeux dans le ciel

Frontex confirme qu'elle utilise "un ensemble de services relevant d'Eurosur, le cadre d'échange d'informations destiné à améliorer la gestion des frontières extérieures de l'Europe" (source : infomigrants.net, "Digital borders : EU increases use of technology to monitor migration", 18.2.2022). Il précise que la majeure partie de cette surveillance est effectuée "par la surveillance aérienne au moyen d'aéronefs pilotés et non pilotés, avec des dispositifs d'imagerie par satellite et la collecte de la position des navires grâce à des systèmes de positionnement".

Selon une récente enquête approfondie ("Funds for Fortress Europe : spending by Frontex and EU-LISA", janvier 2022) réalisée par l'organisation à but non lucratif Statewatch, Frontex consacre la majeure partie de son budget annuel à la surveillance maritime et aérienne, parallèlement aux expulsions (vols affrétés et réguliers pour le retour des migrants). Selon l'analyse des données effectuée par Statewatch, entre 2014 et 2020, Frontex et l'agence européenne EU-LISA (qui supervise les systèmes d'information de contrôle de la mobilité à grande échelle) ont dépensé ensemble 1,9 milliard d'euros en contrats avec des entreprises informatiques privées et l'industrie de la sécurité et de la défense. Sur cette somme, environ un demi-milliard (434 millions d'euros) a été géré par Frontex, dont plus de 100 millions d'euros pour des contrats avec des entreprises privées dans le domaine de la surveillance aérienne. Il s'agissait notamment d'un contrat de 50 millions d'euros avec le consortium

Airbus - l'une des principales entreprises transeuropéennes de l'industrie aérospatiale et de la défense - et la société israélienne Albeit, qui fournit 85% des drones de l'armée israélienne.



https://public.flourish.studio/visualisation/9014574/

Au cours de la même période, Frontex semble avoir entretenu une relation profitable avec trois autres fournisseurs de services de surveillance aérienne : le canadien CAE Aviation, le britannique Diamond-Executive Aviation (DEA) et le néerlandais EASP Air. En tant que consortium, ils ont remporté 8 contrats d'une valeur totale de 57 millions d'euros (sans compter les contrats qu'ils ont signés seuls pour d'autres services de sécurité et de contrôle à Frontex).

La même tendance se poursuit en 2021 avec 84 millions d'euros - soit un sixième du budget annuel de Frontex - consacrés aux services de surveillance aérienne.

Dans le cadre du processus d'expulsion, Frontex a travaillé avec la société polonaise eTravel SA dans le cadre d'un contrat de 30 millions d'euros pour la fourniture de services de voyage (services de réservation et de billetterie) pour les vols de retour réguliers. Elle a également travaillé avec la multinationale britannique Air Charter Service Limited et la norvégienne AS Aircontact pour l'affrètement de vols dans le même but.

L'organisation Privacy International, basée à Londres, a publié en juillet 2021 ses conclusions sur la manière dont un nombre croissant d'entreprises "développent des satellites capables de suivre et de vendre leurs données aux agences frontalières". L'organisation a conclu que si "cette surveillance peut

sauver des vies, elle peut aussi faciliter les retraits ou être utilisée pour persécuter les demandeurs d'asile".

L'utilisation de toutes ces technologies de surveillance a également une conséquence plus profonde, souligne Antonella Napolitano, coordinatrice de réseau de Privacy International. "D'une part, elle contribue à la criminalisation de la personne du migrant, et en même temps elle le transforme en hub de données, depuis le début du voyage du pays d'origine jusqu'à l'évaluation des données biométriques dans l'UE. L'objectif est d'enregistrer intégralement son mouvement et de le suivre jusqu'aux prochaines étapes au sein de l'espace européen. En effet, s'il se retrouve piégé à cause d'un enregistrement ou d'une décision erronée au sein de ces systèmes où sont stockées ses données, cette erreur le suit pour le reste de sa vie."

Cette notion n'est pas sans lien avec le risque d'étendre la surveillance à l'ensemble des déplacements, qu'ils soient touristiques ou professionnels. D'ailleurs, souligne M. Napolitano, "l'interopérabilité même des systèmes est un bon exemple de la manière dont un système développé pour surveiller les mouvements migratoires peut ensuite être étendu à tout le monde, puisque ces systèmes sont progressivement étendus à tous les voyageurs entrant dans l'espace européen, mais aussi aux citoyens de l'UE se déplaçant à l'intérieur de l'UE".

"Le fait d'être potentiellement considéré comme un "criminel par défaut", un concept qui se reflète dans la gestion des technologies de surveillance, ne peut laisser personne indifférent", conclut Mme Napolitano.

Dossier passager : le suivi des mouvements intra-UE

Le Passenger Name Record (PNR) concerne l'enregistrement de toutes les données des passagers se déplaçant sur le territoire européen, qu'ils viennent ou non d'un pays tiers. Que collecte ce système ? Le nom, la nationalité, la date de notre voyage, le lieu de départ et d'arrivée, notre adresse électronique et notre adresse postale. En dehors de cela, on peut connaître nos compagnons de voyage, éventuellement certaines données relatives à notre séjour comme les réservations d'hôtel, si nous avons voyagé pour des raisons professionnelles ou personnelles. Il peut même, dans un cas extrême, connaître notre religion, car le système enregistre même le repas que nous avons pris pendant notre vol. Ce repas peut contenir des informations "intéressantes" sur nous, par exemple, si nous mangeons casher, nous sommes juifs, si nous ne mangeons pas de porc, cela signifie que nous sommes musulmans. Il peut également révéler si quelqu'un a des allergies.

Le PNR est accessible aux autorités de police de chaque pays. "Et c'est là que les problèmes commencent. Il existe une directive européenne sur la manière dont les données à caractère personnel peuvent être traitées par le système PNR. Cette législation européenne doit être transposée dans le droit national de chaque pays. Le problème est que nous avons des échecs dans la transposition de

cette directive dans différents pays, comme la Grèce", explique au MIIR l'avocat Kostas Kakavoulis, membre d'Homo Digitalis. Comme il l'explique, "la directive européenne stipule que chaque État membre établit ou désigne une autorité chargée de la prévention, de la détection, des enquêtes et des poursuites concernant les infractions terroristes graves. Nous parlons donc d'une autorité qui est soit établie dès le départ, soit qui existe et à qui on donne cette compétence. En Grèce, le législateur a confié cette compétence à un département de la direction de la gestion et de l'analyse de l'information de la police grecque. Il ne s'agit donc pas d'une autorité mais d'une direction de la police grecque. Il est absurde que l'organisme qui détient les données, la police, demande l'accès à ces données à un département de la police. S'il est soumis à un contrôle hiérarchique ou s'il existe des pressions en général, il est plutôt douteux qu'un département de la police grecque refuse de fournir à d'autres départements de la police grecque les données dont ils ont besoin, même si cela était nécessaire. En France, ce n'est pas le cas, car une autorité indépendante spéciale a été mise en place pour les données PNR. En Grèce, n'importe quelle force de police peut avoir un accès incontrôlé aux données PNR, partout et à tout moment. Il n'existe aucune trace de qui a demandé quelles données, quand et dans quel but. Et il n'y a pas de politique d'accès classifiée. Il suffit d'être membre de la force de police pour accéder à ces données."

En Grèce, l'organisation Homo Digitalis (membre de l'EDRi), dans une lettre ouverte au Parlement, souligne que "les données en question peuvent révéler le schéma des déplacements d'une personne, comme l'heure du voyage, le lieu de départ et d'arrivée, son adresse électronique et son adresse, ainsi que les compagnons de voyage d'une personne, mais peut-être même les données relatives aux réservations d'hôtel, etc., révélant ainsi des informations sur les voyages d'affaires ou personnels et même le cercle social de la personne, comme ses amis ou ses compagnons".

L'organisation note que dans le projet de loi soumis en 2018 en Grèce, il y avait :

- l'absence d'un système d'enregistrement de l'accès aux données PNR
- l'absence de contrôle judiciaire préalable sur la communication des données PNR aux autorités préjudicielles et autres autorités
- la durée de conservation des données PNR n'est pas limitée à la période strictement nécessaire

Quatre ans plus tard, les mêmes lacunes subsistent.

L'organisation a souligné que les données PNR des mineurs transférés doivent être décrites de manière claire et précise, et que les données transférées ne doivent révéler ni les convictions religieuses ni les informations sur la santé du passager.

Automatisation et surveillance dans la forteresse Europe

Résumé : L'intelligence artificielle et les algorithmes sont au cœur du nouveau régime de contrôle de la mobilité de l'UE. Des décisions automatisées à haut risque sont prises sur des vies humaines. Il s'agit d'un marché émergent non réglementé de plusieurs milliards d'euros avec des applications "intelligentes" dystopiques.

Auteur : Kostas Zafeiropoulos, Ioanna Louloudi, Nikos Morfonios (MIIR)

Lien : Disponible à partir du 26 avril 2022

Texte :

Fin juin 2020, Robert Williams, un résident afro-américain de Détroit, a été arrêté à l'entrée de sa maison, devant ses deux jeunes filles. Personne n'a pu lui dire pourquoi. Au poste de police, il a été informé qu'il était considéré comme un suspect dans le braquage d'un magasin en 2018, car son visage avait été identifié par les images de surveillance de la sécurité du magasin. L'identification était basée sur une ancienne photo de permis de conduire. Après trente heures de garde à vue, Robert Williams a finalement été relâché. Les aveux cyniques des policiers de Détroit sont désarmants : "l'ordinateur a probablement fait une erreur".

Un incident similaire s'est produit en juin 2019 pour Michael Oliver, également un résident afro-américain de Détroit, qui a été arrêté après l'identification présumée de son visage sur une vidéo de caméra de sécurité. Il a été traduit en justice, où il a finalement été acquitté trois mois après son arrestation.

De même, lors d'un test du logiciel Rekognition d'Amazon, le programme a identifié à tort 28 membres du Congrès (!) comme des personnes ayant été arrêtées pour un crime. La grande majorité des erreurs d'identification concernaient des Noirs et des Latinos. Mais ne croyez pas que cela n'arrive qu'aux États-Unis.

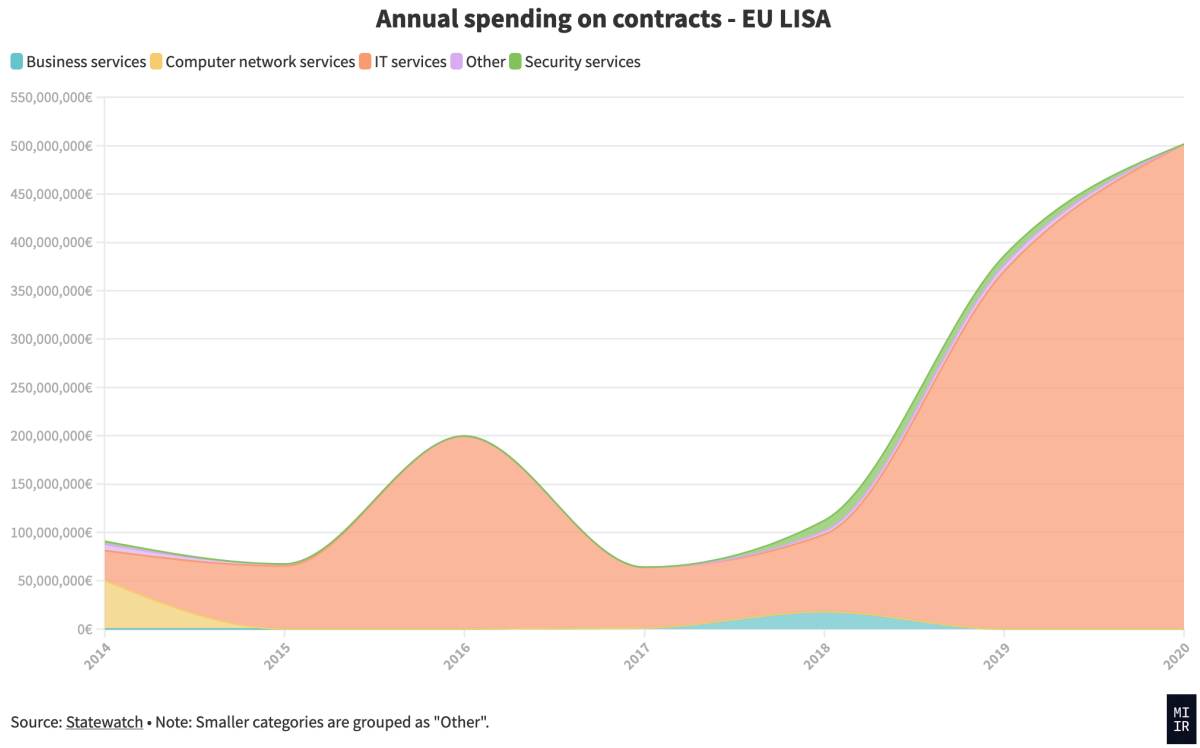
Comme nous l'avons vu dans les deux parties précédentes de la recherche MIIR sur "Les murs de la forteresse numérique de l'Europe", l'UE, dans le cadre d'une nouvelle architecture de surveillance des frontières et de contrôle de la mobilité, a introduit ces dernières années un certain nombre de systèmes pour enregistrer et surveiller les citoyens se déplaçant dans l'espace européen. L'UE utilise différents mécanismes de financement pour la recherche et le développement, en mettant de plus en plus l'accent sur les technologies d'intelligence artificielle (IA), qui peuvent également utiliser des données biométriques. Entre 2007 et 2013 (mais avec des projets en cours jusqu'en 2020), le plus pertinent de ces mécanismes était le septième programme-cadre (PC7), suivi d'Horizon 2020. Ces deux programmes ont financé des projets de sécurité de l'UE pour un montant de plus de 1,3 milliard d'euros. Pour la période actuelle 2021-2027, Horizon Europe dispose d'un budget total de 95,5 milliards d'euros, avec un accent particulier sur les questions de "sécurité". Des technologies telles que la prise de décision automatisée, la biométrie, les caméras thermiques et les drones contrôlent de plus en plus les migrations et touchent des millions de personnes en déplacement. La

gestion des frontières est devenue une entreprise rentable de plusieurs milliards d'euros dans l'UE et dans d'autres parties du monde. Selon une analyse de TNI (Border War Series), la croissance annuelle du marché de la sécurité des frontières devrait se situer entre 7,2 % et 8,6 %, pour atteindre un total de 65 à 68 milliards de dollars américains d'ici 2025.

L'expansion la plus importante concerne les marchés mondiaux des données biométriques et de l'intelligence artificielle (IA). Le marché de la biométrie lui-même devrait doubler son chiffre d'affaires, passant de 33 milliards de dollars en 2019 à 65,3 milliards de dollars en 2024. Une part importante du financement est destinée à renforcer les capacités d'EU-LISA (Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurité et de la justice), qui devrait jouer un rôle clé dans la gestion de l'interopérabilité des bases de données pour le contrôle de la mobilité et de la sécurité. Les activités de ce supercalculateur sont financées par :

- Une subvention provenant du budget général de l'UE.
- Une contribution des Etats membres relative au fonctionnement de l'espace Schengen et aux mesures liées à Eurodac.
- Des contributions financières directes des États membres.

Chris Jones, directeur exécutif de l'organisation à but non lucratif Statewatch, suit depuis plusieurs années la piste de l'argent qui part de Bruxelles. Il explique que "les projets EU-LISA sont généralement gérés par des consortiums d'entreprises privées, d'organismes publics et d'universités. Les entreprises privées reçoivent les sommes les plus importantes, plus que les organismes publics." Une récente étude de Statewatch (Funds for Fortress Europe : spending by Frontex and EU-LISA, January 2022) souligne qu'environ 1,5 milliard d'euros ont été dirigés vers des entrepreneurs privés pour le développement et le renforcement d'EU-LISA au cours de la période 2014-2020, la plus forte augmentation ayant eu lieu après 2017 et le pic de la crise des réfugiés.



https://public.flourish.studio/visualisation/9014422/

L'oligopole de la surveillance

L'un des contrats les plus importants signés en 2020, d'une valeur de 300 millions d'euros, a été conclu entre les entreprises françaises Idemia et Sopra Steria pour la mise en œuvre d'un nouveau système d'appariement biométrique (BMS). Ces entreprises remportent souvent de nouveaux contrats car elles ont conclu des accords pour la maintenance des systèmes EES, EURODAC, SIS II et VIS. Les autres entreprises qui ont obtenu des contrats de grande valeur pour des travaux liés à EU-LISA sont Atos, IBM et Leonardo - pour 140 millions d'euros - et le consortium Atos, Accenture et Morpho (devenu Idemia) qui a signé en 2016 un contrat de 194 millions d'euros. Les données recueillies par Statewatch montrent également une coopération - généralement par le biais de coentreprises - dans l'expansion du système EU-LISA avec des entreprises d'intérêts grecs, comme Unisystems SA (détenue par le groupe Quest de l'ancien président de l'Association des industriels grecs Th. Fessa), qui a signé un contrat de 45 millions d'euros en 2019. De même, European Dynamics SA (appartenant à Konstantinos Velentzas) a participé à un contrat de 187 millions d'euros attribué en 2020, et la société luxembourgeoise Intrasoft International SA (appartenant auparavant aux intérêts de Kokkalis) participe avec cinq autres entreprises à un projet de 187 millions d'euros en 2020.

Contracted companies (by contract size) - EULISA

Search...

Company name	Sum of all contracts	Number of contracts	Address
Sopra Steria Benelux SA/NV	604,954,007 €	6	15/23 Avenue Arnaud Fraiteur, Brussels, Belgium
Atos Belgium NV	573,501,690 €	4	DA Vincilaan 5, Zaventem, Belgium
Idemia Identity & Security SAS	302,550,000 €	1	2, place Samuel de Champlain, Courbevoie, France
Accenture NV/SA	271,786,039 €	8	boulevard de Waterloo 16, Brussels, Belgium
Morpho SAS	194,450,000 €	1	11 boulevard Gallieni, Issy-les-Moulineaux, France
ARHS Developments SA	187,000,000 €	1	13 Boulevard du Jazz, Belvaux, Luxembourg
European Dynamics Belgium SA	187,000,000 €	1	15, rue Belliard, Brussels, Belgium
European Dynamics Luxembourg SA	187,000,000 €	1	12, rue Jean Engling, Luxembourg, Luxembourg
European Dynamics SA	187,000,000 €	1	209, Kifissias Ave. & Arkadiou Str, Athens, Greece
Everis Belgique SPRL	187,000,000 €	1	rue de SPA 8, Brussels, Belgium

1 / 5

Source: Statewatch

MI IR

https://public.flourish.studio/visualisation/9468645/

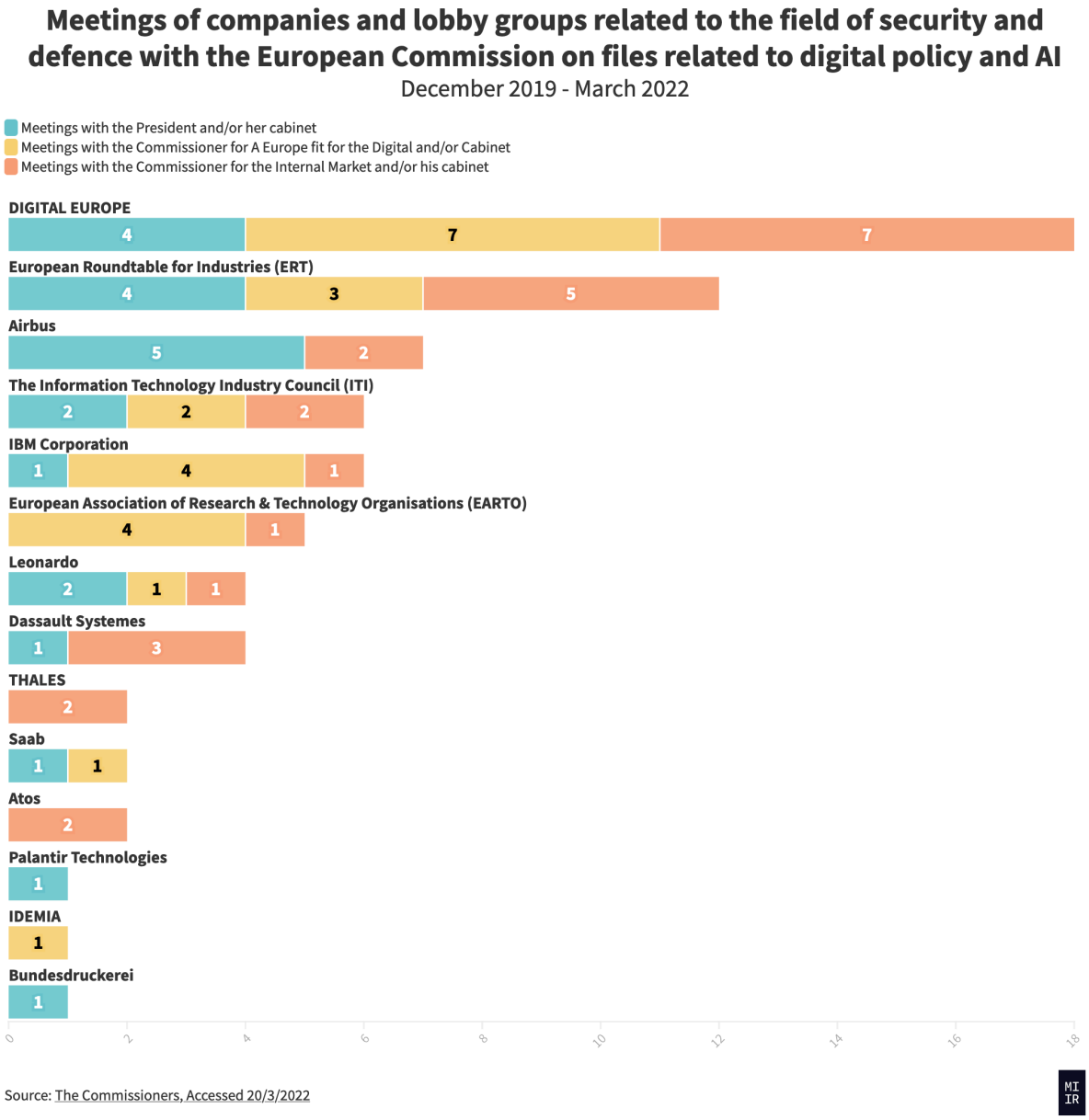
La relation entre EU-LISA et l'industrie est également illustrée par la tenue fréquente d'événements conjoints, tels que la "table ronde avec l'industrie" qui se tiendra le 16 juin 2022 à Strasbourg. Il s'agira de la 15e réunion consécutive de ce type et elle réunira des organes de l'UE, des représentants des systèmes de gestion de la mobilité et des particuliers. "Il y a des négociations étendues, longues et très secrètes entre les États membres et les députés européens chaque fois qu'ils veulent changer quelque chose dans les bases de données. Mais nous ne savons pas quelle est l'influence réelle des entreprises qui gèrent ces systèmes, si elles contribuent à ce qui est techniquement faisable et comment tout cela interagit avec le processus politique", explique Chris Jones de Statewatch. Le contenu des contrats signés entre les consortiums et EU-LISA reste également inconnu, car il n'est pas publié.

La nouvelle frontière de l'IA et les pressions exercées sur l'UE

En avril 2021, la Commission européenne a publié son projet de règlement tant attendu sur l'intelligence artificielle (AI ACT). Le processus de consultation devrait prendre un certain temps. Cet important texte de loi dépasse les 200 pages et qui sera - entre autres - un affinement de la législation sur la protection des données (directive 680/2016). Une pression considérable devrait être exercée par les entreprises et les opérateurs du secteur jusqu'à ce que le projet de loi soit soumis dans sa forme finale au Parlement européen.

Le MIIR a enquêté sur les comptes rendus des réunions officielles sur les questions de politique numérique et d'IA entre la présidente de la Commission européenne Ursula von der Leyen, la

commissaire Margrethe Vestager ("Une Europe adaptée à l'ère numérique"), le commissaire Thierry Breton (marché intérieur) et leurs équipes, entre décembre 2019 et mars 2022. Il ressort qu'au moins 14 agences, géants du secteur privé et consortiums d'entreprises liés au secteur de la sécurité et de la défense ont rencontré des représentants clés de la Commission européenne 71 fois en 28 mois pour discuter de questions liées à la politique numérique et à l'IA. La plupart des réunions avec les commissaires ont été organisées par DIGITALEUROPE, une organisation représentant 78 entreprises membres, dont de grandes entreprises de défense et de sécurité telles qu'Accenture, Airbus et Atos. D'autres consortiums ont également été identifiés comme exerçant un lobbying important, comme la Table ronde européenne des industries (ERT) qui représente un certain nombre d'entreprises de défense et de sécurité telles que Leonardo, Rolls-Royce et Airbus.



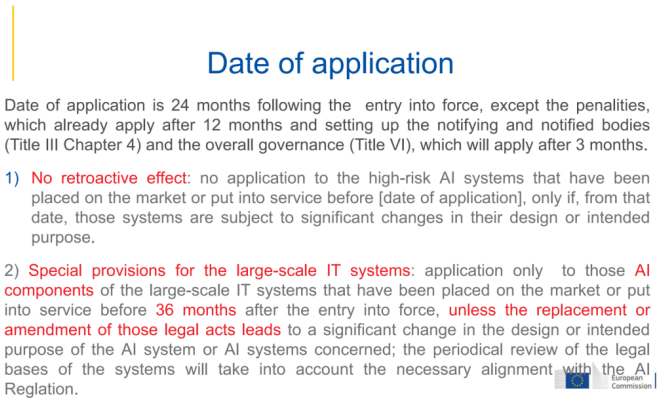
https://public.flourish.studio/visualisation/9083043/

Systèmes à haut risque

La proposition de règlement européen (COM/2021/206 final) adoptée en avril 2021, donne un bon aperçu des systèmes et applications d'IA qui devraient être réglementés, et des risques de leur fonctionnement non réglementé aux points d'entrée de l'Europe. Comme indiqué : "[...] il convient de classer comme à haut risque les systèmes d'IA destinés à être utilisés par les autorités publiques compétentes chargées de tâches dans les domaines de la gestion de l'immigration, de l'asile et du contrôle des frontières en tant que polygraphes et outils similaires ou pour détecter l'état émotionnel d'une personne ; pour évaluer certains risques présentés par des personnes physiques entrant sur le territoire d'un État membre ou demandant un visa ; pour évaluer certains risques présentés par des personnes physiques entrant sur le territoire d'un État membre ou demandant un visa ; pour évaluer le risque des données à caractère personnel d'une personne [...]"

Le paramètre critique

Le champ d'application des systèmes d'IA "à haut risque" semble vaste. Malgré l'espoir qu'une nouvelle directive réglemente leur mode de fonctionnement, un paramètre pourrait supprimer cette possibilité. Comme l'a révélé une présentation interne de la Commission européenne qui s'est déroulée en mai et a été mise en lumière par Statewatch, le nouveau règlement, s'il est adopté, entrera en vigueur 24 mois après sa signature et ne s'appliquera pas à tous les systèmes, car il ne devrait pas être rétroactif pour ceux qui étaient sur le marché avant la date d'entrée en vigueur.



"C'est comme s'il disait clairement : "oui, nous devrions contrôler l'utilisation de l'intelligence artificielle et de l'apprentissage automatique de manière responsable. Mais nous ne le ferons pas pour les systèmes que nous construisons déjà parce que... nous avons d'autres idées pour eux... ", commente Chris Jones. La question est également abordée dans la déclaration commune publiée sous les auspices du réseau des droits numériques EDRI en novembre par 114 organisations de la société civile, soulignant qu'"aucune justification raisonnable de cette exemption de la réglementation sur l'IA n'est incluse dans le projet de loi ou fournie". Dans cette communication, elles appellent le Conseil de l'Europe, le Parlement européen et les gouvernements des États membres à inclure dans le projet de

loi final des garanties en matière de responsabilité qui permettront de garantir un cadre sûr pour la mise en œuvre des systèmes d'IA et, surtout, la protection des droits fondamentaux des citoyens européens.

Les robots-chiens en action : Algorithmes et projets de recherche cauchemardesques

"Les institutions européennes et les États membres déploient de gros efforts pour augmenter le nombre d'expulsions. L'UE a investi de l'argent et des ressources dans ces bases de données pour dire essentiellement "nous voulons aider à retirer ces personnes du sol européen", souligne Chris Jones de Statewatch. En effet, l'automatisation et l'utilisation d'outils algorithmiques poussés par l'industrie jouent déjà un rôle important aux points d'entrée de l'Europe, ce qui soulève de nombreuses questions sur la sauvegarde des droits des réfugiés et des migrants. Ce n'est pas seulement le profilage qui inquiète ceux qui critiquent ces projets européens, mais aussi la qualité des données sur lesquelles ce processus est basé. "Cela ressemble à une "boîte noire", dont on ne sait pas exactement ce qu'elle contient", explique Petra Molnar, spécialiste du droit des réfugiés et anthropologue, qui met l'accent sur le risque d'une automatisation sans facteur humain dans la prise de décision lorsqu'elle détermine des vies humaines.

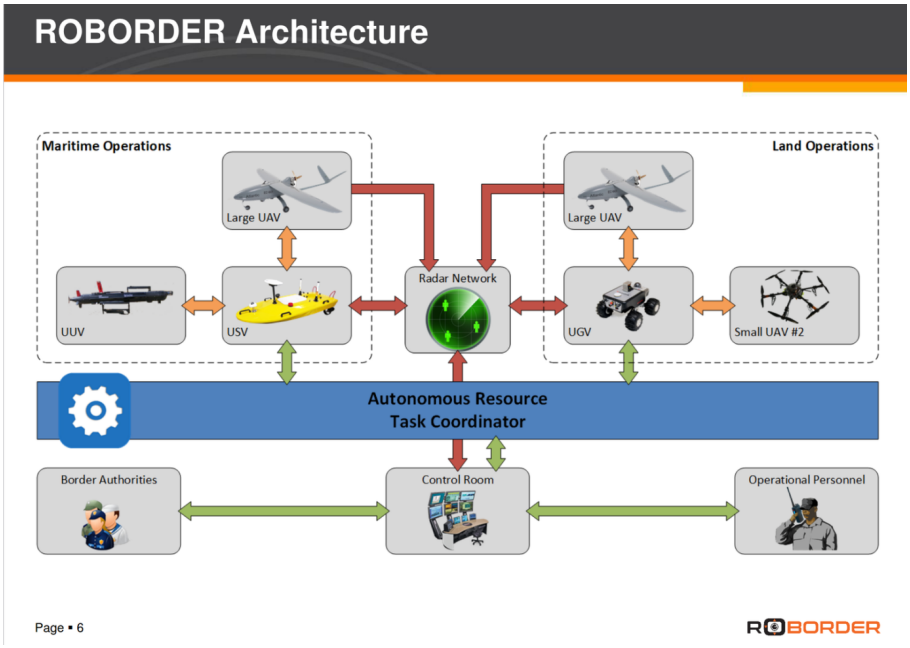
Voici quelques-uns des principaux systèmes pilotes financés au cours des dernières années :

iBorderCtrl - Détecteurs de mensonges "intelligents" : Combine des outils de comparaison faciale et d'authentification de documents avec des technologies d'IA. Il s'agit d'un "détecteur de mensonges", testé en Hongrie, en Grèce et en Lettonie, et impliquant l'utilisation d'un "garde-frontière virtuel", personnalisé en fonction du sexe, de la nationalité et de la langue du voyageur - un garde posant des questions via un appareil photo numérique. Le projet a été financé à hauteur de 4,5 millions d'euros par le programme Horizon 2020 de l'Union européenne, et a été fortement critiqué comme étant dangereux et pseudo-scientifique ("Sci-fi surveillance : Europe's secretive push into biometric technology", The Guardian, 10 décembre 2020 ; "We Tested Europe's New Lie Detector for Travelers - and Immediately Trigger a False Positive", The Intercept, 26 juillet 2019).

Il a été piloté dans des conditions simulées début juillet 2019 dans les locaux de TRAINOSE, dans une zone spécialement conçue du Centre d'études de sécurité d'Athènes. Avant le départ, le voyageur devait télécharger la photo d'une pièce d'identité ou d'un passeport sur une application spéciale. Ils répondaient ensuite aux questions posées par un garde-frontière virtuel. Un logiciel spécial enregistrait leurs paroles et les mouvements de leur visage, qui auraient pu échapper à l'attention d'un œil ordinaire, et au final, le logiciel calculait - soi-disant - le degré de sincérité du voyageur.

Le 2 février 2021, la Cour de justice des Communautés européennes a statué sur un procès intenté par l'eurodéputé et activiste Patrick Breyer (Parti pirate) contre la confidentialité de ce projet de recherche, qu'il a qualifié de pseudo-scientifique et d'orwellien.

Roborder (un essaim autonome de robots hétérogènes pour la surveillance des frontières) : Ce projet vise à développer un système autonome de surveillance des frontières à l'aide de robots sans pilote, notamment des véhicules aériens, maritimes, sous-marins et terrestres. L'ensemble de la plateforme robotique intègre des capteurs multimodaux dans un réseau interopérable unique. Du 28 juin au 1er juillet 2021, l'essai pilote final du projet, auquel participe le ministère grec de la défense nationale, a eu lieu en Grèce.



Foldout : Le projet de recherche Foldout, doté de 8,1 millions d'euros, ne cache pas ses objectifs : "ces dernières années, l'immigration clandestine a augmenté de façon spectaculaire et n'est plus gérable avec les systèmes existants". L'idée principale du projet, piloté en Bulgarie et en cours de déploiement en Finlande, en Grèce et en Guinée française, est de placer des capteurs de mouvement sur les sections terrestres de la frontière où le terrain ou la végétation rend difficile la détection d'un passage irrégulier. À tout mouvement suspect, humain ou véhicule, il sera possible d'envoyer un drone à cet endroit ou d'activer des caméras au sol pour une surveillance supplémentaire. Le consortium qui le développe est coordonné par l'Institut autrichien de technologie (qui a reçu 25 millions d'euros de 37 projets européens).

Parmi les organisations qui font pression pour ces projets au niveau européen, nous avons rencontré EARTO, un consortium de centres de recherche et de bénéficiaires de projets dans divers domaines, dont la sécurité. Parmi eux, KEMEA en Grèce, la Fraunhofer-Gesellschaft (140 projets de recherche financés par l'UE, dont Roborder) et l'Institut autrichien de technologie (Foldout).

Bon nombre des projets de recherche Horizon 2020 (Roborder, iBorderCtrl, Foldout, Trespass, etc.) ont été décrits par leurs propres auteurs comme étant encore "immatures" pour une utilisation généralisée. Cependant, le changement global de l'approche de l'Union européenne concernant l'utilisation de l'IA pour le contrôle de la mobilité et la prévention de la criminalité est visible dans le financement toujours plus important du Fonds européen de sécurité. L'un de ces projets consiste à fournir à la police grecque des milliers d'appareils mobiles qui permettront d'identifier les citoyens à l'aide d'un logiciel de reconnaissance faciale et d'empreintes digitales. Le coût total du projet, entrepris par Intracom Telecom, dépasse les 4 millions d'euros et 75 % proviennent du Fonds européen de sécurité.

L'"expérience" de Samos

"Les frontières et l'immigration sont le laboratoire parfait pour les expériences. Des conditions opaques, à haut risque, avec un faible niveau de responsabilité. Les frontières deviennent le terrain d'essai parfait pour les nouvelles technologies qui peuvent ensuite être utilisées à plus grande échelle sur différentes communautés et populations. C'est exactement ce que l'on voit en Grèce, non ?", demande l'avocate Petra Molnar. La réponse est affirmative, tant pour le nord que pour le sud du pays.

Sur l'île de Samos, à la frontière sud-est de la Grèce avec la Turquie, dans le nouveau camp de migrants dont le gouvernement grec fait presque la publicité, deux systèmes pilotes spéciaux appelés YPERION et KENTYROS sont mis en service.

YPERION est un système de gestion de l'asile répondant à tous les besoins du Service d'Accueil et d'Identification. Il traite les données biométriques et biographiques des demandeurs d'asile, ainsi que des membres d'ONG visitant les structures concernées et des travailleurs de ces structures. Il est prévu qu'il soit l'outil principal du fonctionnement des Centres d'Accueil Fermés (C.A.F.) car il sera chargé du contrôle d'accès, du suivi des prestations par demandeur d'asile utilisant une carte individuelle (nourriture, fournitures vestimentaires, etc.) et des déplacements entre les C.A.F., et les structures d'hébergement. Le projet comprend la création d'une application pour téléphone mobile qui fournira des informations personnalisées à l'utilisateur, qui servira de boîte aux lettres électronique pour sa demande d'asile, avec la possibilité de fournir des informations personnalisées.

KENTYROS est un système numérique de gestion de la sécurité électronique et physique autour et à l'intérieur des locaux, utilisant des caméras et des algorithmes d'analyse comportementale de l'IA. Il comprend une gestion centralisée depuis le ministère de la gouvernance numérique et des services tels que : la signalisation d'alarmes de violation du périmètre à l'aide de caméras (capables de thermométrie, de mise au point et de rotation) et d'algorithmes d'analyse du mouvement ; la signalisation d'alarmes de comportement illégal pour des individus ou des groupes d'individus dans des zones de rassemblement à l'intérieur de l'établissement ; et l'utilisation de systèmes d'aéronefs sans pilote pour évaluer les incidents à l'intérieur de l'établissement sans intervention humaine.

"KENTYROS utilise des caméras qui ont une grande capacité à se concentrer sur des individus spécifiques, des caméras qui peuvent également prendre la température de quelqu'un. Le plus important n'est pas que KENTYROS utilisera cette image pour des raisons de sécurité, c'est que des algorithmes d'analyse comportementale seront également utilisés, sans expliquer exactement ce que cela signifie", déclare l'avocat et membre d'Homo Digitalis, Kostas Kakavoulis. Comme il le souligne, "un algorithme apprend à tirer certaines conclusions sur la base de certaines données que nous lui avons fournies. Un tel algorithme sera capable de distinguer le fait que la personne X a un comportement agressif accru, qu'elle peut attaquer d'autres demandeurs d'asile ou des gardes, ou qu'elle peut vouloir s'échapper illégalement du centre d'hébergement. Une autre utilisation des algorithmes d'analyse du comportement est l'analyse du mensonge, qui permet de juger si notre comportement et nos paroles reflètent quelque chose de vrai ou non. Cela se fait principalement par l'analyse des données biométriques, les données que nous produisons tous par notre mouvement dans l'espace, par notre présence physique, par notre apparence physique et aussi par la façon dont nous bougeons nos mains, la façon dont nous clignons des yeux, la façon dont nous marchons, par exemple. Tout cela peut sembler insignifiant, mais si quelqu'un peut les collecter sur une longue période et les corréler avec les données de nombreuses autres personnes, il peut être en mesure de tirer des conclusions sur nous, qui peuvent nous surprendre, sur l'agressivité de notre comportement, notre degré d'anxiété, notre peur, si nous disons la vérité ou non." Dans la législation actuelle, il est interdit de traiter des données personnelles sans possibilité d'intervention humaine.

L'avocate Petra Molnar a récemment mené des recherches sur les effets des applications de l'IA sur le contrôle des flux migratoires. Elle était à Samos lors de l'inauguration du nouveau centre d'accueil fermé. "De multiples couches de barbelés, des caméras partout, des stations d'empreintes digitales à la porte tournante, des points d'entrée-sortie. Les réfugiés le voient comme un complexe carcéral. Je n'oublierai jamais cela. La veille de l'ouverture, j'étais dans l'ancien camp de Vathi, à Samos. Nous avons parlé à une jeune mère originaire d'Afghanistan. Elle poussait sa petite fille dans un landau et s'empressait de taper un message sur son téléphone : "Si nous allons là-bas, nous allons devenir fous". Et chaque fois que je regarde les camps équipés de ces systèmes, je réalise qu'ils incarnent cette peur que les gens ont lorsqu'ils vont être isolés, et que les technologies de surveillance sont utilisées pour contrôler davantage leurs mouvements."

Médecins Sans Frontières a décrit la nouvelle structure de Samos comme un "cauchemar dystopique". Ils n'étaient pas les seuls. "Le système KENTYROS est encadré par l'utilisation de technologies très intrusives pour protéger la vie privée, les données à caractère personnel ainsi que d'autres droits, comme des algorithmes d'analyse du comportement et du mouvement, des drones et des caméras de surveillance en circuit fermé. Il existe une sérieuse possibilité que l'installation des systèmes YPERION et KENTYROS viole la législation de l'Union européenne sur le traitement des données à caractère personnel et les dispositions de la loi 4624/2019 ", souligne l'ONG Homo Digitalis.

L'Association hellénique des droits de l'Homme, HIAS Grèce, Homo Digitalis et un maître de conférences à l'Université Queen Mary de Londres, le Dr Niovi Vavoula, ont déposé le 18 février 2022 une demande auprès de l'Autorité grecque de protection des données (DPA) pour l'exercice de pouvoirs d'enquête et l'émission d'un avis sur la fourniture et l'installation des systèmes. Le mercredi 2 mars 2022, l'Autorité a ouvert une enquête sur le ministère de l'Immigration et de l'asile en relation avec les deux systèmes en question.

Le fétichisme de l'automatisation

"Le problème est que les autorités, et les politiciens, commencent à percevoir les analyses de données avancées comme des facteurs d'une sorte de connaissance objective et impartiale des questions de sécurité, car elles ont cette aura de précision mathématique. Mais l'intelligence artificielle et l'apprentissage automatique peuvent en fait reproduire et amplifier très précisément les biais du passé. Nous devrions nous rappeler que des données de mauvaise qualité ne feront que conduire à de mauvaises décisions automatisées et biaisées", déclare le chercheur George Glouftios.

---

[1] Ceux-ci ont été résumés ; les descriptions complètes sont disponibles dans le document de la convention de subvention.

[2] Au début du projet, il s'agissait de : (1) le consentement éclairé ; (2) la commercialisation des données ; et (3) les questions de sécurité/cybersécurité.

[3] Disponible sur : http://guidelines.panelfit.eu/understanding-data-protection/

[4] Publication sur Facebook : 159 personnes atteintes ; Premier tweet : 811 impressions, 2 J'aime, 1 retweet ; Second tweet : 1 841 impressions, 6 J'aime, 7 retweets ; bulletin d'information de l'ECSA, juillet 2020 : 438 ouvertures (21,9% des abonnés) ; liste de diffusion de l'ECSA de plus de 600 personnes et organisations.

[5] Le guide PANELFIT sur la recherche et l'innovation responsables fournit de plus amples informations à ce groupe.

[6] Art. 21 de la directive 2013/33/UE (directive refonte des conditions d'accueil). Voir : https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_search/vulnerable-person_en

[7] Bien que ce guide se concentre sur l'Europe, de nombreux types de vulnérabilité sont observés ailleurs. Dans le même temps, d'autres causes et types de vulnérabilité se retrouvent en dehors de l'Europe.

[8] Par exemple, les "réfugiés" sont un groupe vulnérable, mais "être pauvre" et "être sans abri" sont une description de l'état d'une personne à un moment donné et dans un contexte donné.

[9] Il s'agit de lesbiennes, gays, bisexuels, transgenres, queers, intersexes et asexuels.

[10] Voir : www.theguardian.com/world/2020/may/19/hungary-votes-to-end-legal-recognition-of-trans-people

[11] Les Samis sont le seul peuple européen figurant sur la liste des peuples autochtones de l'ONU.

[12] Voir : www.iwgia.org/en/sapmi.html

[13] Il existe des outils gratuits en ligne qui permettent d'analyser l'épilepsie photosensible ; voir, par exemple, www.w3.org/TR/WCAG20-TECHS/G15.html ; le site Web de Mozilla comporte également une section sur les solutions d'accessibilité pour les développeurs : https://developer.mozilla.org/en-US/docs/Web/Accessibility/Seizure_disorders.