LES NOTES DE MIGREUROP
N° 12
PREMIÈRE ÉDITION

PHOTOGRAPHIE : **REFOULÉES D'ALGÉRIE, DES PERSONNES MIGRANTES SONT IDENTIFIÉES PAR L'OIM À AGADEZ AU NIGER, EN 2018.** © FRANCESCO BELLINA

DATA ET NOUVELLES TECHNOLOGIES, LA FACE CACHÉE DU CONTRÔLE DES MOBILITÉS

Décembre 2020

Dans un rapport de juillet 2020, l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle (EU-Lisa) présente l'intelligence artificielle (IA) comme l'une des « technologies prioritaires » à développer. Le rapport souligne les avantages de l'IA en matière migratoire et aux frontières, grâce, entre autres, à la technologie de reconnaissance faciale.

L'intelligence artificielle est de plus en plus privilégiée par les acteurs publics, les institutions de l'UE et les acteurs privés, mais aussi par le HCR et l'OIM. Les agences de l'UE, comme Frontex ou EU-Lisa, ont été particulièrement actives dans l'expérimentation des nouvelles technologies, brouillant parfois la distinction entre essais et mise en œuvre. En plus des outils traditionnels de surveillance, une panoplie de technologies est désormais déployée aux frontières de l'Europe et au-delà, qu'il s'agisse de l'ajout de nouvelles bases de données, de technologies financières innovantes, ou plus simplement de la récupération par les GAFAM des données laissées volontairement ou pas par les migrant·e·s et réfugié·e·s durant le parcours migratoire.

La pandémie Covid-19 est arrivée à point nommé pour dynamiser les orientations déjà prises, en permettant de tester ou de généraliser des technologies utilisées pour le contrôle des mobilités sans que l'ensemble des droits des exilé·e·s ne soit pris en considération. L'OIM, par exemple, a mis à disposition des États sa Matrice de suivi des déplacements (DTM) durant cette période afin de contrôler les « flux migratoires ». De nouvelles technologies au service de vieilles obsessions…

migreurop

Des applications numériques au service de la protection des exilé.e.s ou des frontières ?

Les études sur la « frontiérisation » ont largement porté sur les technologies les plus visibles, telles que les clôtures, les radars ou les drones. Mais de récentes avancées technologiques se sont généralisées avec le prétexte de protéger les exilé·e·s, de leur faire bénéficier d'un service, voire de renforcer leur autonomie. Ces supposées protections ont comme corollaire le contrôle des frontières et, au niveau de l'UE et des États membres, ces technologies fonctionnent comme des dispositifs de « tri social » et d'attribution différenciée des droits.

Dans de nombreux camps à travers le monde, des demandeurs et demandeuses d'asile reçoivent une aide financière mensuelle téléchargée sur des cartes prépayées. Ce qui est présenté par le HCR et les États comme un moyen de favoriser l'autonomie des personnes. Mais ces cartes permettent aussi de les surveiller, via le traçage des retraits au guichet et transactions, et de les contrôler (elles peuvent uniquement acheter ce qui est considéré utile par le HCR et à des commerçant·e·s agré·é·s).

De même, la stratégie du HCR pour l'«inclusion numérique» et l'«identité numérique» des réfugié·e·s repose également sur l'idée du renforcement de leur autonomie, de leur participation à la vie économique et sociale, et de la protection contre la fraude à l'identité. En Jordanie, depuis 2016, le scanner de l'iris pour identifier les demandeurs et demandeuses d'asile dans le camp de Zaatari aurait été conçu par IrisGuard pour « protéger l'identité » des réfugié·e·s, leur garantissant un « statut civil », mais contribue de fait aussi à les contrôler. En effet, le système communique automatiquement avec la base de données d'enregistrement du HCR pour confirmer l'identité du bénéficiaire, vérifie le solde du compte auprès de la Jordan Ahli Bank et des Middle East Payment Services, puis confirme l'achat.

Des applications telles que WhatsApp, Viber, Skype, Facebook ne sont pas à première vue perçues comme des technologies de contrôle. Ce sont pourtant des outils d'extraction de données, qui ne sont pas seulement déployés par les garde-frontières, la police ou les autorités chargées de l'asile, mais de plus en plus utilisés par le HCR ou l'OIM. La surveillance et le contrôle par le biais de ces technologies sont imperceptibles, en grande partie parce que les circuits d'extraction des données restent très largement méconnus.

Si la société civile dans son ensemble connaît très mal les risques qui pèsent, à travers ces applications, sur la protection de la vie privée et des données personnelles, les exilé·e·s sont plus sévèrement impacté·e·s : d'une part parce que, moins encore que les autres, ils n'ont la possibilité de donner un quelconque consentement sur la collecte des données ou leur utilisation. D'autre part parce que leur sort dépend étroitement de l'usage de ces outils numériques. Ainsi, lorsque les applications sont défaillantes, la connexion inexistante ou lorsque les appels n'aboutissent pas, le risque d'exclusion des exilé·e·s de l'accès aux droits, y compris de l'aide humanitaire, est d'autant plus fort.

La réglementation en matière de protection de la vie privée a certes permis de limiter en partie l'utilisation des technologies numériques. Ainsi lorsque l'EASO (European Asylum Support Office) a tenté d'utiliser les réseaux sociaux pour surveiller les itinéraires migratoires, il a été contraint de faire marche arrière. Mais il n'est pas encore possible de demander des comptes aux agences ou aux acteurs privés (comme Microsoft, Accenture, Leonardo, etc.) dans le domaine migratoire, et notamment sur la manière dont ils utilisent les technologies à la frontière, dans les camps de réfugié·e·s et dans les centres de détention, et leur finalité.

Le Pacte européen asile et migration prévoit certes la mise en place d'un mécanisme de contrôle indépendant afin de garantir le respect des droits fondamentaux pendant les procédures de tri à la frontière. Mais il ne dit rien de la mise en responsabilité sur les opérations d'extraction de données et des technologies déployées aux frontières, tant pendant les procédures de contrôle qu'après celles-ci, ce qui laisse de nombreuses questions en suspens.

Les nouvelles technologies à l'épreuve des usages

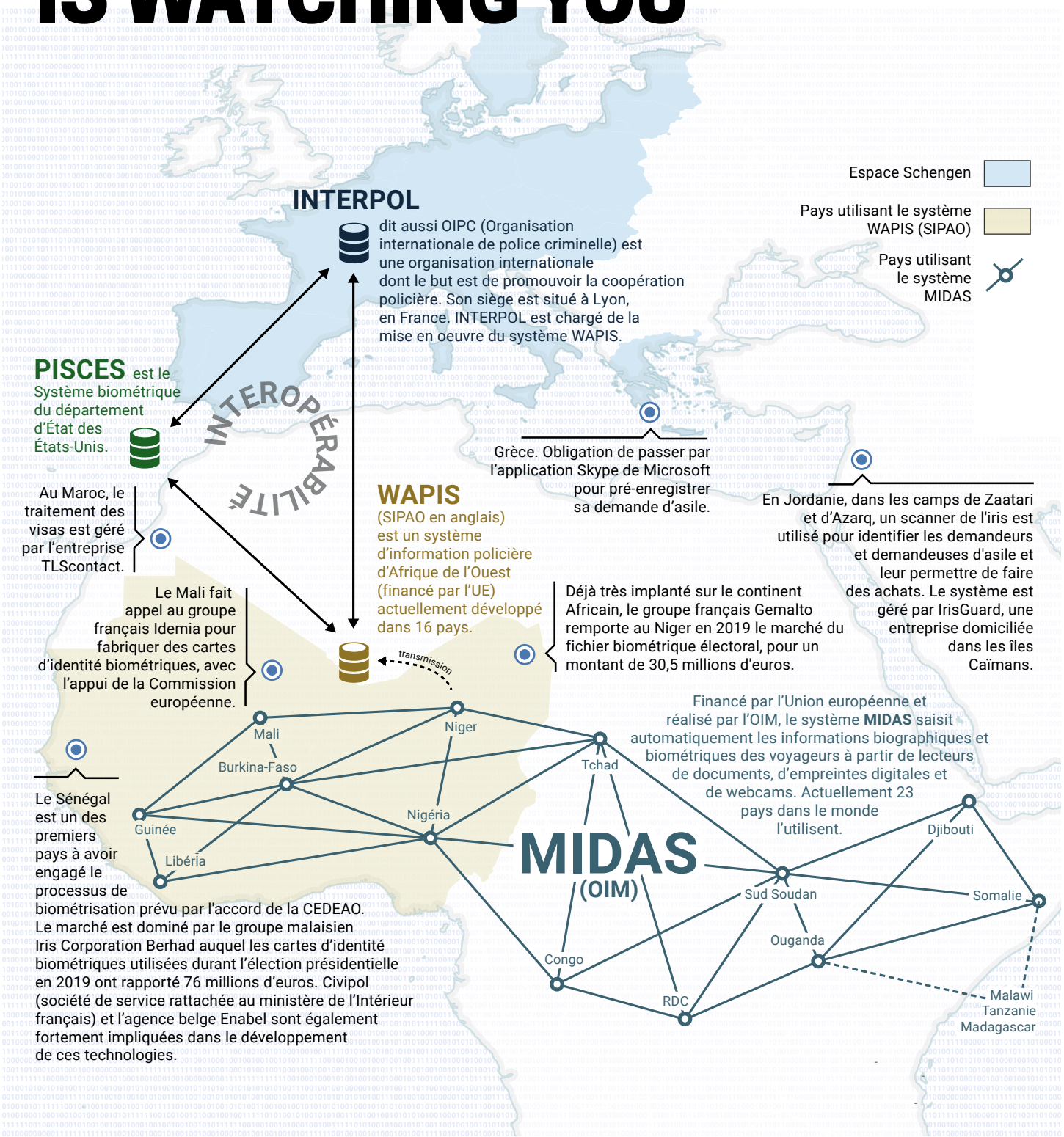
Les avancées technologiques ont transformé le travail des agences humanitaires sur le terrain, avec par exemple l'utilisation de drones pour envoyer du matériel dans des zones inaccessibles, l'utilisation d'imprimantes en 3D pour fabriquer des prothèses, la collecte d'échantillons biométriques (empreintes dentaires ou digitales, ADN) dans le cadre du travail médico-légal pour retrouver l'identité de victimes. Si dans ce dernier cas, l'échantillon collecté est anonymisé avant envoi à un laboratoire, le travail des agences humanitaires requiert généralement un enregistrement des données des personnes pour mener à bien leur mission (état civil, coordonnées, situation familiale, système d'identification de l'iris, etc.). Un profilage et un suivi des personnes qui pourraient se révéler catastrophiques si elles venaient à tomber entre de mauvaises mains.

Cet enjeu de taille préoccupe les agences humanitaires dont certaines, notamment le CICR, plaident pour la création d'un « espace humanitaire numérique » leur donnant un niveau de protection internationale suffisant.

En revanche, ce n'est pas le cas des institutions nationales et des agences européennes comme Frontex qui recourent ouvertement aux nouvelles technologies, dont la biométrie, afin de contrôler les mobilités humaines. Les données récoltées alimentent des bases de données sur les demandes d'asile comme Eurodac, dont l'utilisation n'est pas circonscrite à ce domaine, par exemple si ces données permettent de confirmer l'identité d'une personne avant son expulsion.

Par ailleurs, l'interopérabilité des bases de données, encadrée par deux règlements du 14 mai 2019, est venue compléter le dispositif en renforçant les possibilités de croisement des données enregistrées. L'Union européenne exerce également un droit de regard, via Frontex, sur le système d'information et d'analyse de données sur la migration, installé à Makalondi au Niger (Midas). Un rapport de Privacy International montre, en outre, que le Fonds fiduciaire d'urgence pour l'Afrique de l'Union européenne a financé des systèmes d'identité biométriques au Sénégal et en Côte d'Ivoire, et servi à identifier des personnes « sans-papiers » résidant en Europe et à organiser leur expulsion.

BIG DATA IS WATCHING YOU



Sources :

Mediapart, *Au Niger, l'UE mise sur la police locale pour traquer les migrants*, 28 février 2019

Brochure OIM, *Un système d'information efficace et abordable pour la gestion des frontières*, 2018

Site d'Interpol, *programme WAPIS*

Mediapart, *Au Mali, Niger et Sénégal, le marché de l'identité en plein essor*, 5 mars 2019

Le Monde Diplomatique, *Les réfugiés, une bonne affaire, payer en un clin d'œil*, mai 2017

World Food Programme, *WFP Introduces Innovative Iris Scan Technology To Provide Assistance To Syrian Refugees In Zaatari*, 6 octobre 2016

Socialnetlink, *L'UE finance l'état civil du Sénégal avec une technologie biométrique de 28 millions d'euros pour identifier et faciliter les expulsions*, 23 novembre 2020

Les plateformes numériques et l'humanitarisme financier

Alors que le rôle des sociétés privées et industrielles qui interviennent en matière migratoire commence à être connu, celui des acteurs financiers et des sociétés de haute technologie reste nébuleux, opaque.

En 2016, la Commission européenne a financé et mis en œuvre en Grèce un programme d'assistance financière pour les personnes en demande de protection sous la forme d'aides mensuelles téléchargées sur des cartes prépayées, parrainé par MasterCard (90 euros par mois pour une personne seule ou 150 euros si la personne est dans un centre non équipé de cuisine). Le programme est géré par le HCR et l'opérateur financier concerné, Prepaid Financial Services, dont le siège est à Londres. Pour chaque transaction effectuée par les bénéficiaires, ils et elles doivent payer une commission aux banques grecques depuis lesquelles l'argent est retiré. L'opérateur financier retrace les transactions des cartes de ses bénéficiaires et du lieu où celles-ci ont été effectuées. Chaque carte prépayée est associée à un portefeuille financier unique du HCR, et non à un compte bancaire individuel, et les demandeurs et demandeuses d'asile ne peuvent pas y transférer leur propre argent.

En France, l'allocation versée par l'Ofii (Office français de l'immigration et de l'intégration) aux demandeurs d'asile a été remplacée par une carte qui ne permet pas les retraits d'espèces, mais seulement d'acheter des biens dans les magasins qui l'acceptent. Outre que ce système les empêche d'accomplir nombre de gestes de la vie quotidienne (achat de nourriture en petite quantité, de tickets de bus, paiement des loyers à des bailleurs privés…), il est dénoncé par les associations comme vexatoire et principalement destiné à exercer un contrôle accru sur celles et ceux qui sont contraint·e·s de l'utiliser.

En réalité, les cartes prépayées sont également utilisées comme un moyen de « discipliner » les exilé·e·s en introduisant des restrictions sur les produits qu'ils et elles peuvent acheter, ou dans certains cas, en ne leur permettant pas d'utiliser la carte de paiement aux guichets de retrait.

Par ailleurs, l'intégration des technologies numériques dans le régime d'asile pose des questions majeures sur les circuits financiers du « techno-humanitarisme ». Le partenariat de Microsoft avec le HCR, datant de 1999, s'est renforcé au cours des deux dernières années. Des services de Microsoft sont utilisés par les agents du HCR dans le but prétendu d'accélérer les réponses aux urgences humanitaires et de « protéger » les données des réfugié·e·s. C'est le cas par exemple du BIMS dans lequel sont enregistrées les données de 250 000 réfugié·e·s et déplacé·e·s internes, ou encore du Project Profile et de la base de données ProGres, qui enregistre un grand nombre d'informations individuelles telles que le « nombre de personnes présentes dans les camps, leur âge, le taux de mortalité, l'origine géographique, le type de protection dont ils ont besoin, de même que leur statut médical et des détails sur leur alimentation et leur nutrition ». Si ce partenariat est officiel, aucune mention n'est faite des données auxquelles Microsoft peut avoir accès ou qui peuvent être stockées, ni à quelle fin.

En parallèle, des applications comme Viber, WhatsApp et Skype sont désormais largement utilisées par les acteurs étatiques et les agences internationales, tels le HCR et l'OIM, pour communiquer avec les demandeurs et demandeuses d'asile. En Grèce, depuis 2016, pour demander l'asile sur le continent, les personnes sont obligées de prendre rendez-vous avec le service compétent via Skype. Le recours obligatoire à cette application pour enregistrer cette demande d'asile a fait l'objet de nombreuses protestations collectives de la part des demandeurs d'asile à Athènes au cours des trois dernières années. Ces derniers témoignent de lignes toujours occupées et de l'obligation de disposer d'une connexion internet pour passer l'appel, ce qui n'est possible que pendant des plages horaires hebdomadaires spécifiques. Le gouvernement grec a récemment activé un tchat Viber pour tenir informé·e·s les demandeurs et demandeuses de la situation à Lesbos, et les personnes bénéficiant du programme d'assistance ont dû télécharger cette application pour signaler des problèmes techniques liés à leurs cartes prépayées.

Un tel aperçu met en lumière un domaine émergent de l'industrie de la migration qui devrait faire l'objet d'un examen minutieux : ces acteurs « invisibles » qui contribuent (activement) au contrôle et à la gestion des migrations, collectent constamment des données sur les migrant·e·s. Et les informations récupérées, susceptibles d'être conservées, concernent les comportements, les mouvements et les interactions des personnes. Il n'a pas encore été étudié dans quelle mesure ces divers acteurs accèdent aux données et en tirent profit. Mais la crainte d'une surveillance des exilé·e·s via les réseaux sociaux est suffisante pour en pousser certains à dissimuler leur identité. Combien de temps cet « anonymat » sera-t-il encore possible, à l'heure où les téléphones mobiles sont de plus en plus dotés de serrures biométriques avec empreinte digitale ou reconnaissance faciale ?

La bibliographie est disponible sur le site internet de Migreurop : www.migreurop.org dans la rubrique *Publications/Notes.*
http://www.migreurop.org/article3021.html

migreurop

MIGREUROP est un réseau d'associations, de militant·e·s et de chercheuses et chercheurs présent·e·s dans une vingtaine de pays d'Europe, d'Afrique et du Proche-Orient. Notre objectif est de faire connaître et de dénoncer les politiques de mise à l'écart des personnes en migration, en particulier l'enfermement dans des camps, les formes diverses d'expulsion, la fermeture des frontières ainsi que l'externalisation des contrôles migratoires pratiquée par l'Union européenne et ses États membres.
Nous contribuons ainsi à la défense des droits fondamentaux des exilé·e·s (dont celui de « *quitter tout pays y compris le sien* ») et à promouvoir la liberté de circulation et d'installation.

www.migreurop.org

Retrouvez migreurop sur et sur @migreurop

MIGREUROP - CICP - 21ter rue Voltaire 75011 Paris

Photographie : Francesco Bellina - Design graphique : La société
Dir. de la publication : Claudia Charles

AVEC LE SOUTIEN DE :

ccfd-terre solidaire · The Fund for Global Human Rights · Fondation monde un par tous · Fondation Abbé Pierre