Le gouvernement du Canada s’est associé au Forum économique mondial pour imposer un système de type crédit social pour voyager

[Source : guyboulianne.com]

Par Guy Boulianne

Vous vous demandez pourquoi votre gouvernement vous empêche de voyager à l’intérieur ou à l’extérieur du Canada si vous n’êtes pas pleinement vacciné ? C’est qu’il vous trahit au plus haut niveau et qu’il vous enc*le tout aussi profondément. Entre un Justin Trudeau qui vient d’être nommé par António Guterres pour promouvoir le « développement durable » dans le monde par l’ONU et une Chrystia Freeland qui siège au conseil d’administration du Forum économique mondial (FEM) où elle côtoie sur une base régulière son fondateur Klaus Schwab, les Canadiens sont les pauvres victimes d’un complot de haute trahison en vertu du Code criminel canadien (L.R.C. (1985), ch. C-46(2)b). Oui, les gouvernements complotent contre vous. Cela ne veut pas dire que le secret soit nécessaire pour eux puisque, selon le dictionnaire Larousse, comploter équivaut à *« avoir un comportement qui prête à penser qu’on prépare une action dirigée contre quelqu’un, quelque chose ; manigancer »*. Les comploteurs n’ont plus besoin de se cacher comme autrefois car ils sont désormais rendus à l’étape de l’exécution de leurs plans machiavéliques pour vous asservir tous. On vous empêche de voyager car vous êtes des prisonniers à l’intérieur de votre propre pays jusqu’à ce que leur système de contrôle social numérique « à la chinoise » soit dûment implanté sur le sol canadien.

Sachez que les politiciens véreux n’en ont rien à foutre de vous. Ils n’en ont rien à foutre de la Constitution de votre pays. Ils n’en ont rien à foutre de votre vie ou de votre mort. Tout ce qu’ils veulent est de servir la Bête de l’événement et ainsi acquérir une miette de pouvoir. Mais ils s’apercevront que cette miette de pouvoir se délaiera rapidement et qu’il ne leur restera que le vide d’une coque sans âme.

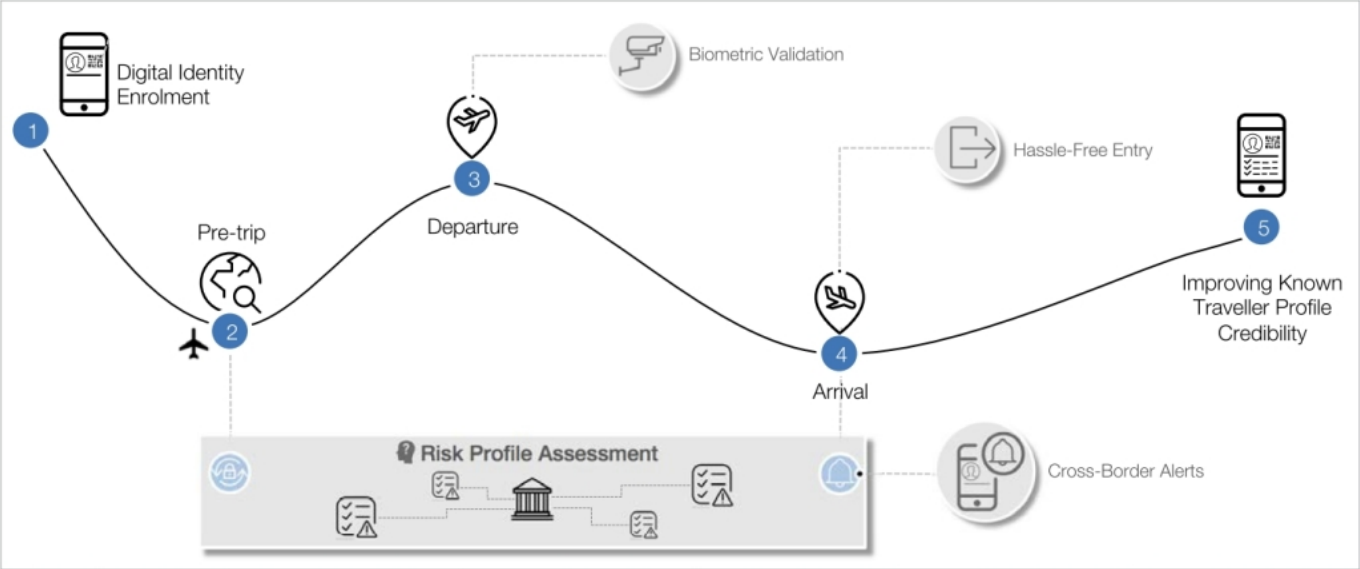
En effet, le gouvernement du Canada, Air Canada et deux grands aéroports canadiens se sont associés au Forum économique mondial (FEM) sur un projet d'identification numérique qui pourrait nécessiter un système de type crédit social pour voyager. Ce projet est connu sous le nom "Known Traveler Digital Identity" (Identité numérique du voyageur connu). *« Le groupe pilote, convoqué par le Forum économique mondial, est composé du gouvernement du Canada et des Pays-Bas, d'Air Canada, de KLM Royal Dutch Airlines, de l'aéroport international Montréal-Trudeau, de l'aéroport international Pearson de Toronto et de l'aéroport d'Amsterdam Schiphol »*, écrit le FEM. Le KTDI est considéré comme un moyen de *« promouvoir des voyages de passagers sûrs et fluides en prévision de l'évolution des comportements et des attentes des voyageurs, du besoin critique de renforcer la sécurité transfrontalière et de l'augmentation du nombre de passagers attendue au cours de la prochaine décennie »*. Le site Web affirme qu'il est basé sur une « identité numérique décentralisée » qui permettra aux gouvernements de confirmer la preuve de citoyenneté et d'autres aspects de l'identité. Chaque fois qu'un gouvernement vérifie l'identité numérique (digital ID) d'une personne, elle est ajoutée à son dossier, ce qui peut affecter son statut.

Known Traveler Digital Identity (KTDI) est une vision de « surveillance par conception » pour le suivi et le contrôle des voyageurs plus dystopique que tout ce que nous avons vu auparavant. KTDI utiliserait un registre distribué basé sur une chaîne de blocs pour relier, via une application sur l'appareil mobile d'un voyageur, toutes les données suivantes :

- Biométrie (initialement des images faciales, éventuellement aussi des empreintes digitales, etc.) ;
- Pièces d'identité émises par le gouvernement (numéro de passeport, etc.) ;
- Historique des voyages, y compris les journaux des passages frontaliers,

des séjours à l'hôtel et éventuellement des locations de voitures et/ou d'autres événements ;
- Journaux d'achat et éventuellement informations sur les comptes bancaires et/ou autres enregistrements financiers et de transaction ;
- « Évaluation des risques » prédictifs et scores de profilage générés à chaque point « d'intervention » avant et pendant chaque voyage ou transaction.

Chaque séjour à l'hôtel, achat ou autre transaction deviendrait comme un passage frontalier estampillé de manière permanente dans votre passeport dans le cadre d'un « laissez-passer de voyage » numérique soumis à une inspection sur demande par les autorités aux points d'« intervention » ultérieurs. Toutes ces données sont destinées à être utilisées pour discriminer les voyageurs dont les profils pré-criminels liés à l'identité sont classés comme « à haut risque » ou « à faible risque » :



L'accès à un historique de voyage et à des journaux de transactions plus complets est un objectif de longue date des agences gouvernementales de surveillance et de contrôle des voyages. Conformément aux normes établies par l'OACI, un espace est réservé sur la puce RFID de chaque passeport électronique pour les données d'historique de voyage. Mais cela était destiné, pour autant que nous puissions en juger, uniquement aux données de passage des frontières ou d'entrée / sortie, et non aux journaux de séjours à l'hôtel ou à d'autres transactions. À notre connaissance, peu de pays ont enregistré des données d'historique de voyage sur des puces RFID de passeport, probablement en raison de l'espace limité réservé dans la structure des données et des complications liées à la modification ou à l'ajout en toute sécurité des données sur la puce une fois qu'elle est écrite pour la première fois et signé numériquement par le gouvernement émetteur.

Lors d'une présentation à la conférence *Hotel Electronic Distribution Network Association* (HEDNA), des représentants d'Accenture (le maître d'œuvre du FEM pour le projet KTDI) et Marriott se sont vantés de la façon dont, sur la base des données KTDI, un individu pouvait être choisi parmi une foule pour «

liste noire » utilisant la reconnaissance faciale automatisée, « *sans arrêter ni reconnaître la caméra* ». Il peut donc être utilisé pour une surveillance de masse subreptice et non consensuelle.

Les partenaires du projet KTDI incluent des agences gouvernementales (DHS, OACI, INTERPOL, etc.) et les industries aériennes et informatiques des compagnies aériennes (IATA, Amadeus, etc.). Mais ce n'est pas tout. Parmi les autres partenaires du projet KTDI figurent Google (Google a acquis un fournisseur de système de réservation informatisé en 2010, mais on ne sait pas à quel titre Google participe au projet KTDI), les chaînes hôtelières Marriott and Hilton (basées aux États-Unis) et Accor (basées en France), et la société de traitement des paiements et des cartes de crédit Visa.https://www.youtube.com/embed/hyFLmnb2xHM?version=3&rel=1&showsearch=0&showinfo=1&iv_load_policy=1&fs=1&hl=fr&autohide=2&wmode=transparent

La dystopie totalitaire du Forum économique mondial devient réalité

En janvier 2018, un projet pilote de surveillance des voyageurs aériens, commandé par le Forum économique mondial, a été approuvé à Davos.

A l'époque, l'économiste Norbert Häring présentait le projet *Known Traveler Digital Identity* (KTDI) comme une « dystopie totalitaire ». Un rapport de suivi montre que les multinationales associent avec succès les gouvernements et l'UE à leurs plans. Le Covid-19 accélère considérablement la mise en œuvre et Bill Gates nous fait savoir par inadvertance comment.

À l'instar du rapport de 2018 intitulé "The Known Traveller: Unlocking the potential of digital identity for secure and seamless travel" (Le voyageur connu : Libérer le potentiel de l'identité numérique pour un voyage sécurisé et fluide), ce livre blanc plus technique de KTDI intitulé "Known Traveler Digital Identity Specifications Guidance" (Guide des spécifications d'identité numérique des voyageurs connus) a été publié sans fanfare sur Internet, en mars 2020. Ces rapports, préparés par le cabinet de conseil Accenture, sont destinés à être lus uniquement par des personnes du secteur de la surveillance et de la sécurité numériques. Pour des raisons compréhensibles, ces personnes préfèrent parler d'identité numérique plutôt que de contrôle ou de surveillance numérique.

Voici comment le schéma KTDI est censé fonctionner : nous téléchargeons des informations nous concernant dans une base de données – ou autorisons d'autres à le faire. Tout d'abord, cela devrait être une preuve d'identité des autorités, mais aussi nos antécédents de voyage, les données bancaires, les chambres d'hôtel, les réservations de voitures de location, les documents des universités, des bureaux gouvernementaux et bien plus encore. Si nous voulons franchir une frontière, nous donnons préalablement aux autorités accès à cette base de données, afin qu'elles puissent voir à l'avance que nous sommes inoffensifs. Grâce à la reconnaissance faciale et à notre smartphone (idéalement) biométriquement lié, ils peuvent nous reconnaître au passage de la frontière. Si nous avons été suffisamment diligents dans la fourniture de données, nous serons autorisés à contourner les files d'attente des autres voyageurs, bénéficiant d'un traitement préférentiel et de contrôles minimaux. Toutefois, comme il est indiqué dans le premier rapport KTDI, en cas de doute sur les intentions d'un voyageur, l'agent des frontières peut, sur la base des informations fournies à l'avance, poser à la personne concernée des questions plus approfondies, par exemple *« pour mieux comprendre ses activités récentes »*.

On peut facilement imaginer à quel point cette diffusion des données sera « volontaire » une fois le système mis en place. Ce sera du genre : vous pouvez librement choisir si vous voulez entrer dans le pays et remettre la clé de vos données, ou si vous préférez rester à l'extérieur. Un essai est déjà en cours par les autorités frontalières du Canada et des Pays-Bas, avec les compagnies aériennes KLM et Air Canada dans les aéroports d'Amsterdam, de Toronto et de Montréal.

Les entreprises participantes, telles que Visa et Google, ne développent pas un tel système pour les autorités policières à leurs propres frais uniquement par sens du devoir cosmopolite. Le rapport KTDI 2018, ainsi que le livre blanc actuel, indiquent tous deux que l'autosurveillance à la frontière sert à créer une masse critique de participants à la norme de partage de données interopérable à l'échelle mondiale qui doit être introduite.

Les autorités frontalières sont simplement le catalyseur idéal d'un système mondial de surveillance de masse assistée par les citoyens et de partage de données, impliquant progressivement tous les gouvernements du monde. Une fois que les États-Unis et quelques autres grands pays auront pris part à ce programme, les citoyens d'un pays dont le gouvernement refuse de participer auront de grandes difficultés à voyager à l'étranger.

Une fois que tous les gouvernements auront adhéré à cette norme pour l'échange volontaire forcé de données avec les citoyens, il est prévu que nous serons également autorisés à transmettre nos données dans les interactions quotidiennes avec les entreprises et les autorités. Dans les deux rapports, la santé, l'éducation, la banque, l'aide humanitaire et les élections sont les domaines mentionnés.https://www.youtube.com/embed/cnUAQKKnEAU?version=3&rel=1&showsearch=0&showinfo=1&iv_load_policy=1&fs=1&hl=fr&autohide=2&wmode=transparent

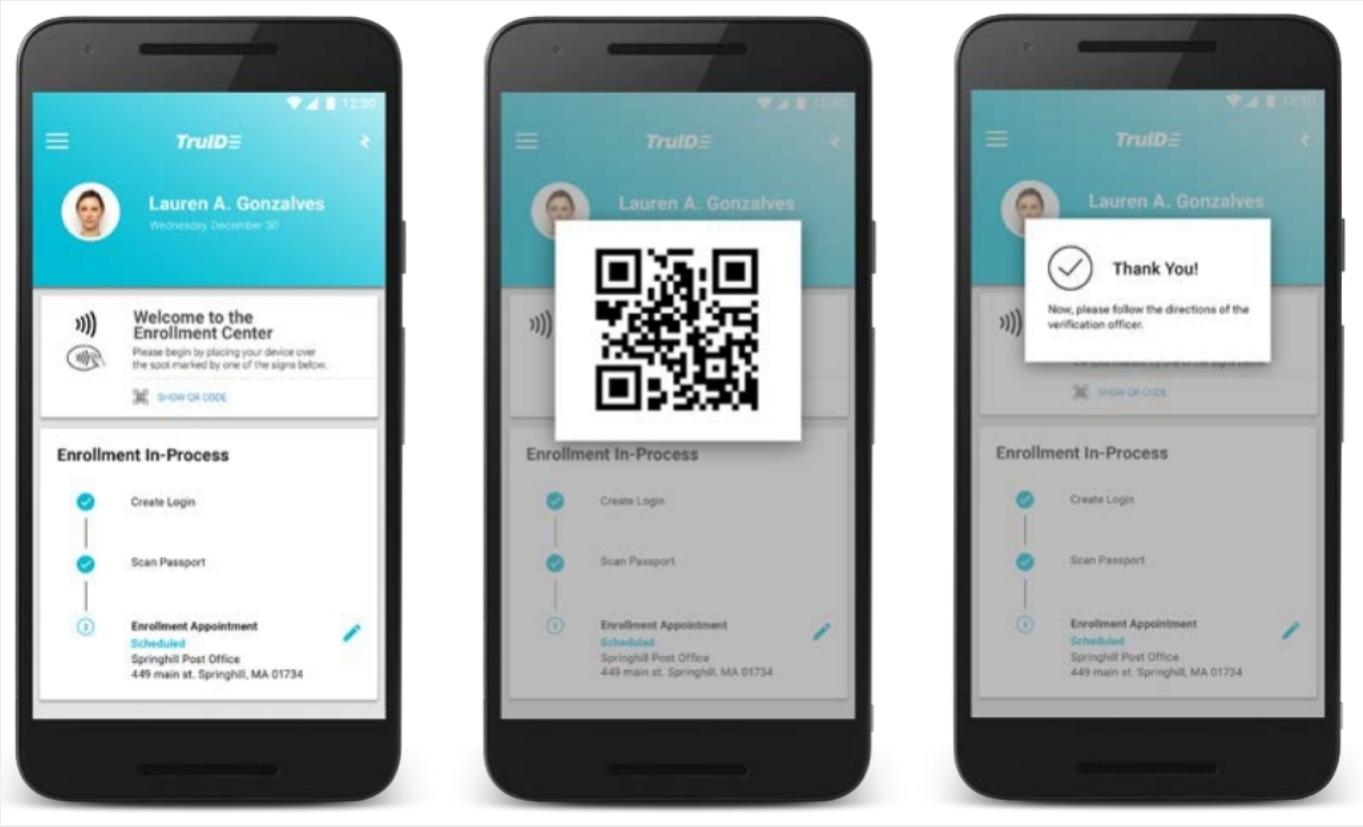
Un système global et totalitaire

Le livre blanc de KTDI précise la grande ambition du projet dans ses conclusions :

> « Ce document décrit l'ambition de KTDI de fournir les bases d'un écosystème d'identité décentralisé accepté à l'échelle mondiale. Un développement plus poussé et une adoption plus large dépendent de la maximisation de l'interopérabilité des échanges de données et de la confiance fédérée. Le succès reposera sur la coopération entre les gouvernements mondiaux, les régulateurs, l'industrie aéronautique, les fournisseurs de technologie et d'autres acteurs pour établir des normes et des spécifications mondiales pour la conformité de toutes les parties prenantes. »

Les conditions d'application de cette norme mondiale de surveillance sont excellentes. Le projet *Known Traveler* utilise des normes techniques pour les informations d'identification vérifiables et les identifiants décentralisés tels qu'ils sont actuellement développés par le *World Wide Web Consortium* (W3C). Le W3C est l'organisme de normalisation le plus important pour l'Internet et est dominé par les entreprises américaines d'Internet et de télécommunications.

Les membres du W3C recoupent fortement ceux de la *Decentralized Identity Foundation*, que des multinationales telles que Microsoft et de nombreuses petites entreprises du secteur de la sécurité numérique ont fondée pour faire progresser les normes mondiales de contrôle d'identité. Les entreprises qui composent ce groupe ont souvent des liens très étroits avec la communauté du renseignement. US Homeland Security a été impliqué dans le projet *Know Traveler* depuis le début. Lors des forums d'identité numérique pertinents, des représentants d'entreprises des industries de l'identité et de la sécurité numériques se mêlent aux représentants de toutes les agences de sécurité et de renseignement concernées.



Volontariat forcé

L'astuce est la fiction du volontariat, le consentement explicite, s'il est extorqué, à l'utilisation des données, que vous devez donner chaque fois que vous souhaitez recevoir un service gouvernemental dans ce système ou si vous souhaitez simplement payer quoi que ce soit par voie numérique. Ceci est similaire à ce qui vous arrive si vous vous déplacez sur le World Wide Web aujourd'hui. Vous devez constamment accepter volontairement de surveiller les demandes des opérateurs du site Web ou simplement choisir de rester à l'écart.

Le système mondial envisagé a un aspect particulièrement pernicieux, qui tourne en dérision l'autonomie et le contrôle souvent annoncés de ceux qui sont supposés posséder leurs données :

> « Les attributs d'identité sont attestés et fournis par les autorités émettrices (c'est-à-dire le numéro de passeport, les coordonnées bancaires). Une autorité émettrice peut également révoquer un VC (identifiant virtuel) qu'elle avait précédemment émis en mettant à jour l'accumulateur cryptographique basé sur la blockchain en conséquence. »

Imaginez à quoi cela ressemblera lorsque ce système sera mis en place comme prévu dans le monde entier, dans tous les pays, aussi répressifs soient-ils. Supposons que l'abolition de l'argent liquide – qui est menée en parallèle par plus ou moins le même groupe d'entreprises et d'agences – soit menée à bien. Pour tout ce que vous voulez faire ou payer, vous dépendez de la

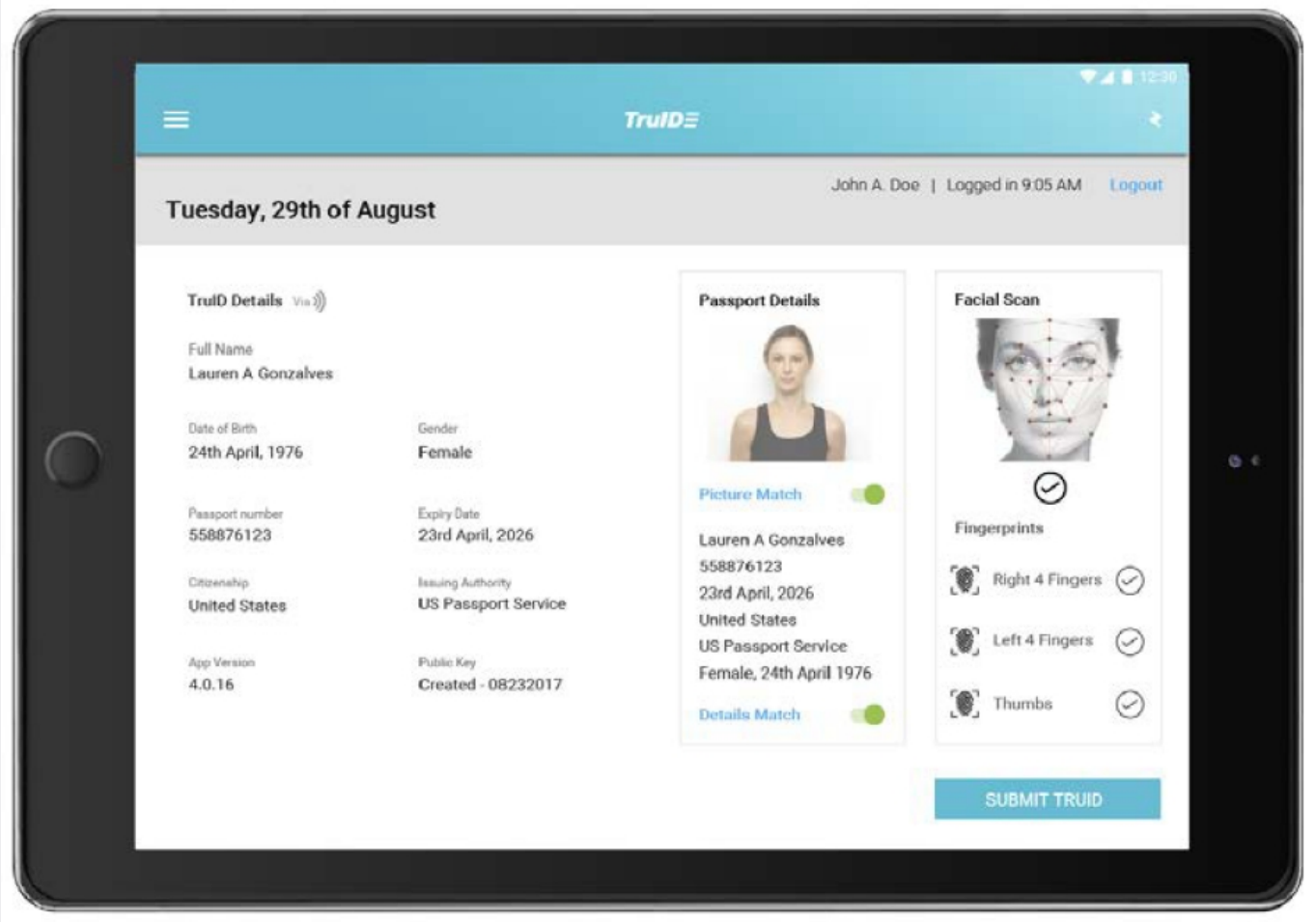
présence d’une coche aux bons endroits dans la base de données sur vous. Si vous tombez en disgrâce auprès de votre propre gouvernement, il pourrait supprimer la coche de vos informations d’identité et vous visser, même si vous n’êtes pas dans le pays. Votre banque peut faire de même.

Si cela vous arrive, vous pouvez essayer de continuer pendant un certain temps. Mais finalement, vous devrez peut-être faire ce que le héros de la science-fiction “Soleil à crédit” de Michel Grimaud (1975) a dû faire. Lorsque sa carte électronique, dont tout le monde avait besoin pour se déplacer et se nourrir, a été confisquée par l’un des guichets automatiques, il s’est volontairement présenté aux portes de la prison et est resté volontairement en prison jusqu’à sa libération, car sinon il serait mort de faim.

Si le gouvernement américain ou les algorithmes contrôlés par ses agences ont quelqu’un dans le monde en vue, ils peuvent faire la même chose. Soit ils demandent au gouvernement ou aux banques respectifs d’invalider tous les documents numériques de la personne cible, soit les sociétés Internet américaines qui contrôlent le système peuvent le faire, soit les agences privées américaines de notation de crédit réduisent la cote de crédit.

Une grande partie de cela est déjà possible aujourd’hui et se fait, mais pas souvent à des particuliers. Mais le système ne sera complet et parfait que s’il existe une norme technique mondialement acceptée qui permet d’accéder à toutes ces données et documents de n’importe où. Ce n’est qu’alors que Washington (ou plutôt Fort Meade et Langley) pourront contrôler à partir de leurs ordinateurs personnels tout le monde dans tous les coins participants du monde. Dans le même temps, les gouvernements nationaux autoritaires pourront contrôler tout le monde dans leur propre sphère d’influence, qu’ils soient chez eux ou à l’étranger.

C’est l’agenda derrière le travail intense que l’USAID, Gates et le Forum économique mondial font, avec l’aide d’une ONU dépendante, pour créer des identités numériques pour chaque personne sur le globe. Ils travaillent à travers ID4Africa, ID2020 et une douzaine d’autres initiatives et consortiums similaires avec ID dans leurs noms.



Rapport minoritaire rechargé

Tout le monde peut alors être guidé par un anneau nasal normalement imperceptible. Cependant, cela pourrait être brutalement tiré, même si vous n'avez rien fait du tout, simplement parce qu'un algorithme conclut que vous êtes un type qui, statistiquement, pourrait bientôt causer des problèmes, comme dans le film "Minority Report". L'ambition d'y arriver est documentée dans le premier rapport KTDI du Forum économique mondial avec une citation en surbrillance du directeur de Google, Rob Torres :

> « Les entreprises technologiques ont fait des progrès majeurs dans l'exploration de données, l'apprentissage automatique et l'intelligence artificielle permettant une analyse prédictive améliorée. En combinaison avec les informations fournies par les passagers, ces technologies peuvent être utilisées par les gouvernements pour… analyser des modèles complexes de mégadonnées dans le but de prévoir les risques de sécurité aux frontières. »

La citation indique clairement que l'identité numérique ne consiste pas simplement à donner à chacun un moyen facile de prouver qui vous êtes au moyen d'un certificat de naissance numérique ou d'une carte d'identité numérique, comme ils essaient de nous le faire croire. Si vous n'êtes pas encore convaincu, voici une autre citation, extraite du "EU blockchain

observatory report on digital identity and blockchain” (Rapport de l’observatoire de la blockchain de l’UE sur l’identité numérique et la blockchain) :

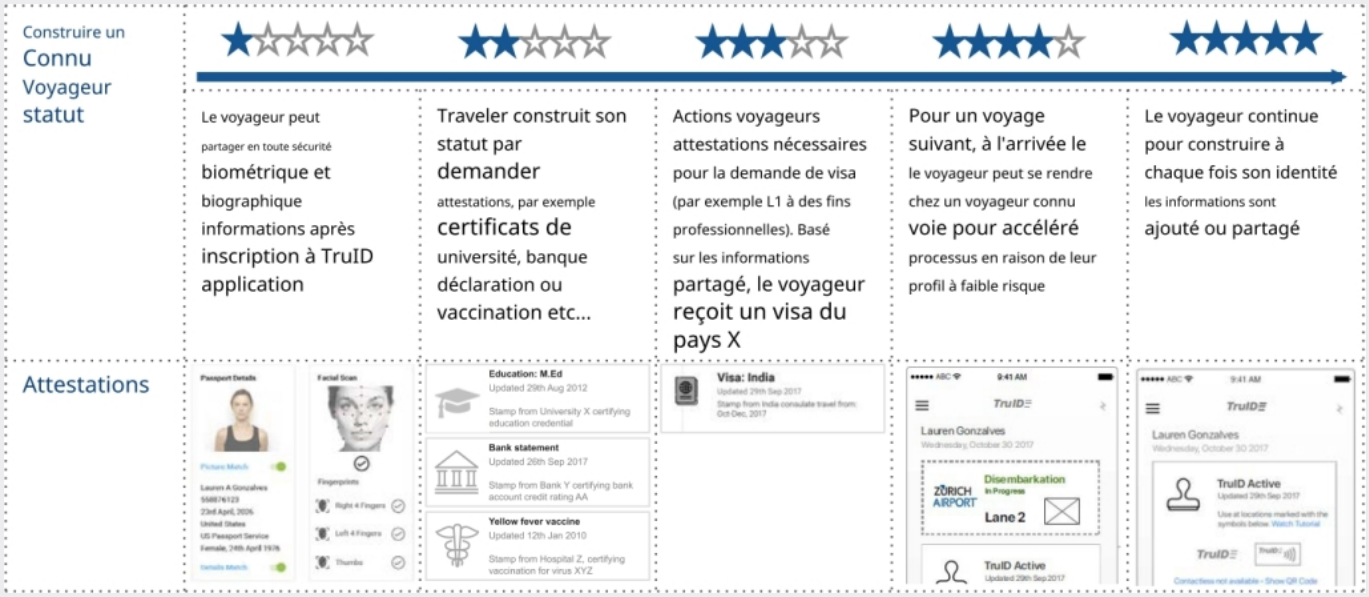
> « Lorsque nous parlons d’identité numérique, nous devons la comprendre comme la somme de tous les attributs qui existent à notre sujet dans le monde numérique, une collection de points de données en croissance et en évolution constantes. »

Ainsi, l’identité numérique signifie tout ce qui peut être stocké numériquement et qu’il y a à savoir sur nous, nos actions et nos préférences. Il s’agit d’introduire tout ce que l’on sait sur une personne dans une base de données qui peut être exploitée par toutes les entreprises et tous les gouvernements participants et manipulée par eux à tout moment. De sorte que les entreprises peuvent nous diriger en tant que bétail de consommation dans le bon corral et nous tondre chacun de nous individuellement et de manière optimale, et nous avoir comme des bêtes de somme peu exigeantes et obéissantes. Il s’agit pour les gouvernements et les entreprises d’être en mesure de détecter très tôt toute personne qui pourrait vouloir sortir du système ou casser le système.

Remarquablement, le Forum économique mondial affirme qu’il n’a pas encore proposé de concept pour la gouvernance de cette infrastructure de contrôle totalitaire mondiale, c’est-à-dire qui devrait être aux commandes de ce système. Le Livre blanc dit :

> « Les travaux sur la définition et le développement d’un cadre de gouvernance approprié pour le concept KTDI se poursuivent et seront abordés dans un prochain rapport. »

En d’autres termes, les gouvernements sont censés s’engager dans ce concept sans que l’on sache qui tirera les ficelles. En réalité, bien sûr, c’est assez clair. C’est Washington et les grandes entreprises américaines, directement ou par l’intermédiaire d’organismes internationaux tels que le Forum économique mondial, le W3C, le GAFI et bien d’autres, qu’ils dominent.



Les gouvernements et l’ONU se sont alignés

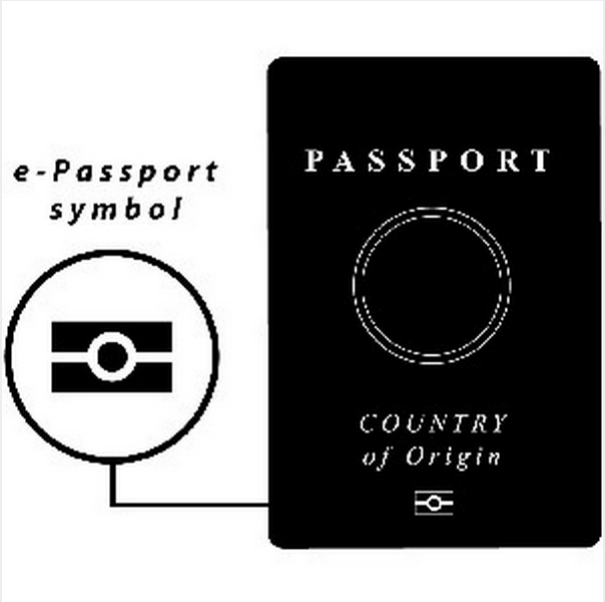
Néanmoins, les gouvernements et une ONU dépendante de l’argent des entreprises semblent très désireux de participer à ce système de surveillance mondial développé par les multinationales et la US Homeland Security. Il est commercialisé par les entreprises participantes de l’industrie de la sécurité et de l’identité sous le nom euphémique d’identité auto-souveraine (SSI).

A Bruxelles, ce terme, SSI, s’impose. Le Comité économique et social européen, un organe de l’UE au sein duquel les associations d’employeurs, les syndicats et d’autres groupes d’intérêt sont censés représenter la « société civile organisée », a élaboré un cadre européen d’identité souveraine (eSSIF). C’est presque un contre un la dystopie décrite dans les rapports du Forum économique mondial.

Les gouvernements de 21 pays, dont l’Allemagne, ont formé un “partenariat européen de la blockchain” trois mois seulement après la réunion du Forum économique mondial de 2018 au cours de laquelle le concept de voyageur connu a été présenté. Ce partenariat semble viser à faire progresser le concept de surveillance du Forum économique mondial dans son incarnation européenne eSSIF. L’un des objectifs de travail de ce partenariat, comme indiqué dans la présentation du Comité économique et social en lien ci-dessus, est de savoir comment préserver les valeurs démocratiques européennes dans la mise en œuvre des SSI. Bonne chance avec ça !

Il existe plusieurs autres groupes et partenariats au niveau européen pour la mise en œuvre du SSID et il existe divers groupes associés aux Nations Unies au niveau mondial. Il devrait déjà être clair que KTDI et SSI ne sont pas des idéaux irréalistes de Washington et des entreprises technologiques, mais un plan réaliste qui est déjà mis en œuvre à l’échelle mondiale.

Le Covid-19 accélère beaucoup les choses



Les réactions des gouvernements à la Covid-19 en Corée du Sud et en particulier à Wuhan, en Chine, et des programmes similaires qui devraient bientôt être mis en œuvre en Occident, accélèrent le glissement mondial vers un contrôle algorithmique total de la population. À Wuhan, si vous ne pouvez pas afficher un bouton vert sur votre smartphone de surveillance qui signale que vous n'êtes probablement pas infecté, vous êtes interdit d'accès à la plupart ou à toutes les formes de transport en commun et vous n'êtes pas autorisé à entrer dans les restaurants ou à vous enregistrer dans les hôtels. En Corée du Sud, les enregistrements des caméras de surveillance, les données des cartes de crédit et les données GPS sont évalués pour identifier et suivre les porteurs potentiels de virus.

Dans une entrevue vidéo du 24 mars 2020, le deuxième homme le plus riche et probablement le plus puissant du monde est interviewé par le modérateur de TED Chris Anderson à propos de la stratégie corona américaine. Dans sa pose de pouvoir décontractée habituelle, Bill Gates parle comme s'il était président des États-Unis ou chef de l'ONU. L'interview devient particulièrement intéressante lorsque Gates en vient à l'immunité présumée des personnes qui se sont déjà remises d'une infection. Gates relie cela à la question de savoir comment et quand les restrictions de voyage peuvent être assouplies :

> « Finalement, nous devrons avoir un certificat indiquant qui est une personne récupérée, qui est une personne vaccinée, parce que vous ne voulez pas que des gens se déplacent dans le monde où vous avez certains pays, qui ne le contrôleront pas, malheureusement. Vous ne voulez pas bloquer complètement la capacité de ces personnes à aller et revenir et à se déplacer. »

Et puis vient la phrase doublement intéressante :

>

> « Il y aura donc éventuellement ce type de preuve d'immunité numérique, qui facilitera la réouverture mondiale. »

Cette dernière phrase est doublement intéressante à cause du mot « numérique » et parce que la phrase n'est contenue que dans une version légèrement plus longue de la vidéo que quelqu'un a téléchargée pour la préserver. Dans la vidéo officielle de TED, cette phrase a été coupée (à la minute 34:27). Selon les commentaires sous la vidéo plus longue, cela s'est produit dans l'après-midi du 31 mars. C'est étonnant, car la seconde moitié de la phrase sur la réouverture des frontières est en fait une très bonne conclusion sur ce sujet, avant que l'intervieweur ne pose la question suivante. On ne le couperait pas pour des raisons journalistiques. La couper par souci de brièveté n'aurait pas beaucoup de sens, car elle ne dure que deux ou trois secondes et la coupure est perceptible.

C'était vraisemblablement le mot « numérique » qui devait être supprimé. Car cela invite à des questions qui mènent finalement à tout ce qui constitue le programme *Known Traveler*. Dans ce qui reste de la vidéo officielle, Gates ne parle que d'un certificat. Cela invite à comprendre ce dont il parle : seuls ceux qui ont un certificat d'immunité délivré par une autorité sanitaire peuvent réserver un vol, et seuls ceux qui peuvent le produire peuvent monter à bord d'un avion et passer l'immigration. Ce serait assez facile à mettre en œuvre et relativement sans problème.

Avoir le certificat en version numérique semble plus pratique, car ce serait plus rapide et plus facile. Mais si une preuve d'immunité numérique pour les voyages internationaux doit être (machine-)utilisable à l'échelle mondiale, elle a besoin d'une norme mondiale pour le certificat, d'un emplacement de stockage pour les certificats considéré comme sûr et généralement accessible, d'une norme d'échange de données qui fonctionne partout, et une norme mondiale pour certifier l'authenticité d'une preuve numérique. Le *Known Traveler Program*, piloté par la US Homeland Security et le Forum économique mondial, veut développer et mettre en œuvre tout cela. Bill Gates est l'un des membres les plus influents du Forum économique mondial, sinon le plus influent.

	1.Accès transparent et vérification	2. Plateforme de partage de données	3. Identité numérique du voyageur connu (intervention sélectionnée)
			
La description	Vérification d'identité et octroi d'accès avec un jeton numérique unique pour la preuve d'identité, basée sur la biométrie, pour les entreprises privées de l'écosystème du voyage. Une fois vérifié, le voyageur peut utiliser un seul jeton pour s'identifier dans l'écosystème de partenaires sans identification physique.	Plateforme intégrée de partage de données sur les voyageurs qui permet une meilleure évaluation des risques par les gouvernements grâce au partage des résultats de contrôle (par exemple, feu rouge ou vert). Les moyens existants de vérification de l'identité (un passeport physique) restent inchangés pour améliorer la confiance.	Une identité numérique qui comprend des données biométriques, biographiques et d'historique de voyage permet au voyageur d'autoriser les entités du voyage du voyageur à accéder à des informations sélectionnées à leur sujet pour permettre l'évaluation des risques, la vérification et l'accès.
Avantages	+ Utile pour piloter avec des entreprises privées + Les changements requis à l'écosystème actuel sont limités + Pas de suivi des données personnelles des voyageurs, limitant ainsi les éventuelles contraintes de confidentialité	+ Permet aux gouvernements d'améliorer l'évaluation et la personnalisation des risques + N'oblige pas les gouvernements à faire confiance à une « identité numérique » + Capacité à se concentrer sur les voyageurs potentiels à haut risque	+ Permet au voyageur d'être un partenaire dans le processus de sécurité + Respecte la souveraineté des pays + Intègre la capacité d'entreprendre la vérification et l'évaluation des risques + Permet un partage d'informations structuré et approfondi en amont avec les entités + Risques identifiés grâce à une meilleure opportunité d'exploitation et d'analyse des données par rapport à d'autres bases de données
Les inconvénients	- La technologie n'est pas utilisée pour l'évaluation des risques - Doit s'harmoniser avec les initiatives existantes - Nécessite un accord entre de nombreuses entreprises du secteur privé	- Doit surmonter les problèmes de protection des données/vie privée - Nécessite la confiance dans le système, entre les gouvernements - Risques liés à l'existence de bases de données centralisées	- Nécessite la confiance entre les entités - Les risques pour la vie privée doivent être traités - Le soutien du gouvernement est essentiel au succès
Notation sur la conception des principes	Processus ② ○ Technologie ④ ○ ○ ○ La coopération ② ○	Processus ② ○ Technologie 0 La coopération ② ○	Processus ④ ○ ○ ○ Technologie ④ ○ ○ ○ La coopération ④ ○ ○ ○

Google et Apple viennent à la rescousse

Le 10 avril 2020, Google et Apple ont annoncé qu'ils coopéreraient afin de permettre aux applications de suivi des contacts d'être interopérables sur les systèmes d'exploitation Adroid et iOS à partir du mois de mai suivant et de programmer la capacité de suivi dans leurs propres systèmes d'exploitation peu après. La recherche des contacts nécessite que les autorités sanitaires puissent alimenter le système, dont le numéro de téléphone est connecté à une personne testée positivement. Celui-ci peut facilement être complété en cochant la case convalescence ou vaccination. Et voila, le programme *Known Traveler* est prêt dans une première application.

Et comme il se doit, le volontariat, la souveraineté sur ses propres données (Self-Sovereign Identity) est totalement préservée. Chacun peut décider par lui-même s'il veut voyager et utiliser l'application de suivi ou s'il préfère rester à la maison.

Étant donné que Google et Apple travaillent de toute façon en étroite collaboration et en toute confiance avec les autorités de sécurité et les services secrets, il ne sera pas difficile d'ajouter d'autres domaines d'application. Tout d'abord, les autorités de sécurité peuvent cocher la case « ne peut pas voyager » ou « à surveiller » si nécessaire. Encore plus intéressant, la fonction de suivi des contacts peut être utilisée pour établir un réseau de contacts de personnes à surveiller et pour ajouter ces contacts à la liste. Au-delà de cela, le système pourrait être affiné davantage selon les besoins dans le sens de ce qui est décrit dans les rapports Known Traveler qu'Accenture a produits pour le FEM.

Grâce à la Covid-19, le Brave New World prend forme bien plus rapidement qu'on ne l'aurait cru. Et grâce à la Covid-19, beaucoup ou même la plupart des gens trouveraient actuellement un tel pouvoir totalitaire souhaitable. La Covid-19 est un cadeau du ciel pour les plans du Forum économique mondial.https://www.youtube.com/embed/y_GFx1uXdhk?version=3&rel=1&showsearch=0&showinfo=1&iv_load_policy=1&fs=1&hl=fr&autohide=2&wmode=transparent

---

TÉLÉCHARGEMENT DES RAPPORTS DU KNOWN TRAVELER DIGITAL IDENTITY :

- Security in Travel: Promoting Seamless and Secure Travel through Cross-Border Data Sharing and Collaboration, March 2016. – [FRANÇAIS]
- Digital Borders: Enabling a secure, seamless and personalized journey. – [FRANÇAIS]
- Known Traveller: Unlocking the potential of digital identity for secure and seamless travel. – [FRANÇAIS]

SOURCES ET RÉFÉRENCES :

- Keean Bexte : « Canada is a partner in WEF's program to bring digital ID to travel ». The Counter Signal, April 14, 2022.
- Edward Hasbrouck : « "Known Traveler Digital Identity" (KTDI) ». Papers, Please! The Identity Project, March 30, 2020.
- Transports Canada : « Le gouvernement du Canada mettra à l'essai des technologies de pointe favorisant la sûreté et la fluidité des déplacements des voyageurs aériens dans le monde entier ». Gouvernement du Canada, 25 janvier 2018.
- Norbert Häring : « The Totalitarian Dystopia of the World Economic Forum is Becoming Reality ». Money and more, April 11, 2020.
- Edward Hasbrouck : « RFID passport logo (or « mark of the beast »?) ». The Practical Nomad, Wednesday, 1 February 2006.

- WUHAN, China (AP) : « Chinese smartphone health code rules post-virus life ». Associated Press, April 2, 2020.
- Analysis : « World Economic Forum consortium launches Known Traveller Digital Identity paperless travel pilot between Canada and the Netherlands ». Corporate Travel Community, 2 July, 2019.
- Biometrics Topics : « Known Traveller Digital Identity (KTDI) – biometrics topics ». Biometrics Research Group, Inc.
- Forum économique mondial : « Le consortium du Forum économique mondial lance le premier projet pilote de voyage sans papier entre le Canada et les Pays-Bas ». Cision, 26 juin 2019.
- Josh K. Elliott : « Canada leading pilot project for trusted traveller smartphone app ». CTVNews.ca, February 12, 2018.
- Keean Bexte : « FEATURE: Why is a digital ID so dangerous? ». The Counter Signal, April 14, 2022.
- Edward Hasbrouck : « Governments prepare to log travellers’ movements on passport chips ». The Practical Nomad, Thursday, 28 September 2006.