Russie : Edward Snowden dénonce une loi « Big Brother » et la « surveillance de masse » en Russie

	Edward Snowden dénonce une loi « Big Brother » et la « surveillance de masse » en Russie

Edward Snowden, l'ancien agent du renseignement américain réfugié en Russie, a dénoncé samedi 25 juin les lois antiterroristes adoptées par les députés russes. Ces dernières relèvent selon lui de « Big Brother » et de la « surveillance de masse », et a demandé qu'elles ne soient pas promulguées.

« La nouvelle loi russe Big Brother constitue une violation inapplicable et injustifiable des droits qui ne devrait jamais être promulguée », a écrit sur Twitter le lanceur d'alerte, qui a fui les Etats-Unis pour révéler l'ampleur de la surveillance menée par les services de renseignement américains.
« La surveillance de masse ne marche pas. Ce texte va coûter de l'argent et de la liberté à chaque Russe sans améliorer la sécurité », a-t-il insisté dans un second message.

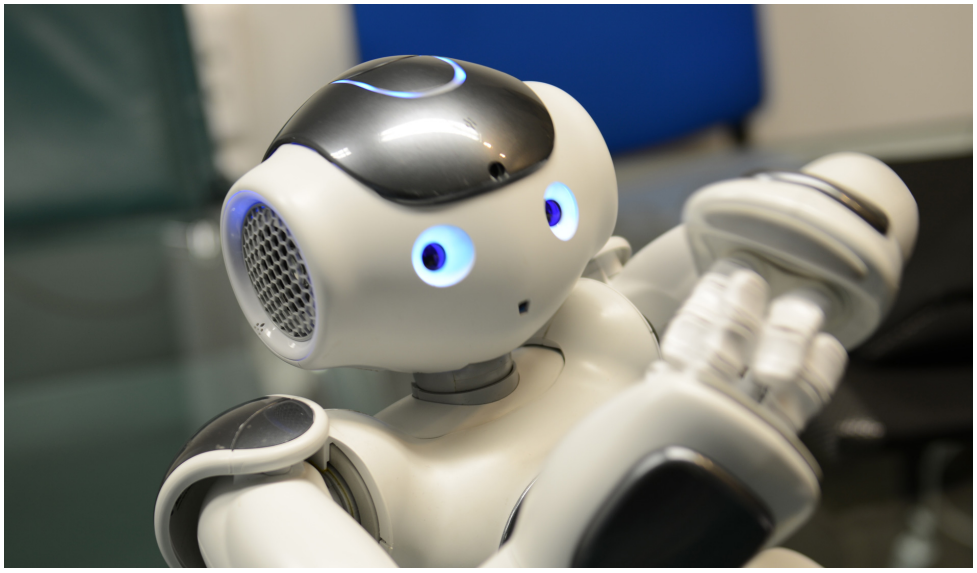
Des lois extrêmement répressives

Adoptés vendredi lors de la dernière séance de la Douma (chambre basse) avant les législatives du 18 septembre, les projets de loi en question obligent en particulier les opérateurs de télécommunications et internet à stocker les messages, appels et données des utilisateurs pendant six mois pour les transmettre aux *« agences gouvernementales appropriées »* à leur demande.
Les réseaux sociaux se voient également obligés de stocker les données pendant six mois, selon l'un de ces textes qui doivent encore être approuvés par le Conseil de la Fédération (chambre haute) et promulgués par M. Poutine.
Ce délai de six mois *« n'est pas seulement dangereux, il est inapplicable »*, a prévenu M. Snowden, qui avait été critiqué, par le passé, pour ne pas critiquer assez sévèrement le régime de Vladimir Poutine.
Ces lois ont été dénoncées par l'opposition russe comme une tentative de *« surveillance totale »* de la part des autorités, mais aussi par les entreprises du numérique qui ont critiqué un coût exorbitant.
Elles introduisent par ailleurs des peines de prison pour la non-dénonciation d'un délit, abaissent l'âge de la responsabilité pénale à 14 ans et introduisent des peines allant jusqu'à sept ans de détention pour la*« justification publique du terrorisme »*, y compris sur internet.
Article original Le Monde

Réagissez à cet article

Original de l'article mis en page : Russie : Edward Snowden dénonce une loi « Big Brother » et la « surveillance de masse »

Faut-il que les robots et les Intelligences Artificielles payent des cotisations sociales ?



Faut-il que les robots et les IA payent des cotisations sociales ?

Comment financer la sécurité sociale lorsque les employés mis aux chômage par les robots ne versent plus de cotisations ? Pour Mady Delvaux, auteure dun projet de résolution qui sera débattu au Parlement européen, il est temps de faire cotiser les robots.

Faut-il reconnaître un droit spécifique des robots ? La commission du Parlement européen en charge des affaires juridiques (JURI), qui a établi un groupe de travail sur la robotique et l'intelligence artificielle, le pense. Elle prépare actuellement un rapport rédigé par l'eurodéputée luxembourgeoise Mady Delvaux (S&D), déposé le 31 mai dernier, qui demande à la Commission d'élaborer une proposition de directive sur des règles de droit civil sur la robotique. Le texte n'a pas encore été adopté en commission JURI, et devrait être débattu en séance plénière du Parlement européen le 12 décembre prochain.
Parmi ses dispositions, la proposition de résolution invite l'exécutif à réfléchir à la manière dont le modèle social européen peut évoluer, alors que « le développement de la robotique et de l'intelligence artificielle pourrait avoir pour conséquence l'accomplissement par des robots d'une grande partie des tâches autrefois dévolues aux êtres humains ».


Mady Delvaux, députée luxembourgeoise au Parlement Européen (groupe Socialistes & Démocrates)

UNE SITUATION PRÉOCCUPANTE POUR L'AVENIR DE L'EMPLOI ET LA VIABILITÉ DES RÉGIMES DE SÉCURITÉ SOCIALE

Actuellement, l'essentiel du financement de sécurité sociale, qu'il s'agisse du socle de base de l'assurance santé, de la retraite ou de l'assurance chômage, est assis sur une ponction d'une partie conséquente des salaires versés aux employés. C'est le salarié chargé de faire l'inventaire dans un hypermarché qui cotise pour être protégé le jour où son employeur jugera plus rentable de faire faire l'inventaire par un robot intelligent.
Paradoxe des paradoxes, l'employeur lui-même complète les cotisations par ses propres versements qui sont proportionnels aux salaires versés, ce qui fait qu'il doit cotiser lorsqu'il continue à payer l'humain (et cotiser d'autant plus lorsqu'il le paye bien), mais qu'il n'a plus rien à payer lorsqu'il le remplace par un robot.

DÉCLARER LES GAINS DE PRODUCTIVITÉ POUR MIEUX LES TAXER ?

Dès lors, si l'on considère que les emplois deviennent plus rapides à détruire qu'à créer dans une société toute obnubilée par l'ubérisation et les gains de productivité, cette « hypothèse s'avère préoccupante pour l'avenir de l'emploi et la viabilité des régimes de sécurité sociale, si l'assiette de contributions actuelle est maintenue », s'inquiète le rapport Delvaux.
L'eurodéputée luxembourgeoise propose donc à la Commission « d'envisager la nécessité de définir des exigences de notification de la part des entreprises sur l'étendue et la part de la contribution de la robotique et de l'intelligence artificielle à leurs résultats financiers, à des fins de fiscalité et de calcul des cotisations de sécurité sociale ». Dit autrement, les entreprises seraient taxées sur la part de leur chiffre d'affaires imputable aux productions automatisées, pour alimenter le pot commun de la sécurité sociale.

UN REVENU UNIVERSEL DE BASE FINANCÉ PAR LES ROBOTS

« Eu égard aux effets potentiels, sur le marché du travail, de la robotique et de l'intelligence artificielle, il convient d'envisager sérieusement l'instauration d'un revenu universel de base », ose même la députée socialiste, alors que la Suisse vient de rejeter la proposition par référendum, et qu'en France le débat est souhaité par Manuel Valls mais sans cesse repoussé.
Mais comment calculer les cotisations que les entreprises devraient reverser ? La question est extrêmement complexe et n'est pas aidée par l'annexe du rapport, où il est simplement précisé que les entreprises devraient être tenues de déclarer à l'administration :
• Le nombre de « robots intelligents » qu'elles utilisent ;
• Les économies réalisées en cotisations de sécurité sociale grâce à l'utilisation de la robotique en lieu et place du personnel humain ;
• Une évaluation du montant et de la proportion des recettes de l'entreprise qui résultent de l'utilisation de la robotique et de l'intelligence artificielle.

Or comment savoir, par exemple, si un rendez-vous enregistré dans l'agenda par Siri ou Cortana est un gain de productivité imposable au titre de la robotisation, parce qu'il aurait pu être inscrit par un(e) secrétaire, ou directement par le patron ou le cadre à travers un logiciel plus ou moins automatisé ? La fiscalité traditionnelle est déjà d'une complexité impressionnante, mais ce n'est rien en comparaison de ce que propose le rapport. Et pourtant, il faudra bien y réfléchir et trouver des solutions. À moins que la crise que nous traversons soit véritablement conjoncturelle et que se créent rapidement de nouveaux emplois durables difficilement remplaçables à court ou moyen terme. « Des emplois qui répondent à des besoins d'humanité », comme le défend le roboticien sud-coréen Jeakweon Han.
Crédit photo de la une : Stephen Chin
Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : Faut-il que les robots et les IA payent des cotisations sociales ? – Politique – Numerama

---

Le gouvernement pourrait partager vos données personnelles avec le secteur pharmaceutique

Le gouvernement pourrait partager vos données personnelles avec le secteur pharmaceutique

---

Selon une information du quotidien De Morgen, le secrétaire d'Etat à la vie privée Philippe De Backer (Open Vld), estime que le gouvernement devrait être en mesure de transmettre des données relatives à la santé des citoyens belges au secteur pharmaceutique. « Nous pourrions demander de l'argent pour cela, à partir du moment où il y a un retour vers le patient », a expliqué De Backer.

Philippe De Backer présente sa note politique « Privacy » au Parlement. Dans celle-ci, il envisage un échange plus large des données personnelles des patients. Selon le secrétaire d'Etat, l'accès aux données et le traitement des données personnelles offrent d'importantes opportunités sociales et économiques. Les données publiques dans le domaine des soins de santé peuvent aboutir à des innovations intéressantes dans le secteur pharmaceutique, notamment en termes de prévention et vice-versa.

Compensation financière et contrôle du partage des données

En échange de ces informations privées, les patients pourraient recevoir une compensation financière. « Nous pourrions demander de l'argent pour cela, à partir du moment où il existe un juste retour pour le patient », a expliqué Philippe De Backer. Ce dernier évoque entre autres des prix moins élevés pour les médicaments des patients.

Par ailleurs, le secrétaire d'Etat souhaite également étendre la marge de manœuvre de la Commission de la vie privée. Celle-ci devrait déterminer quelles entreprises privées pourraient avoir accès aux données personnelles aux mains des pouvoirs publics. La Commission de la vie privée devrait également être en mesure d'infliger des amendes pouvant aller jusqu'à 4% du chiffre d'affaires pour les entreprises qui utilisent de façon inadéquate ces informations personnelles.

Philippe De Backer veut enfin que le patient ait davantage de contrôle sur la manière dont sont utilisées ses données. Dans ce sens, il évoque la création d'un passeport de confidentialité qui permettrait aux patients de savoir qui utilise leurs données personnelles.

Article original de Arnaud Lefebvre

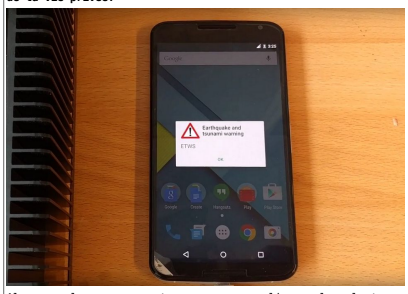
Réagissez à cet article

Original de l'article mis en page : Le gouvernement pourrait partager vos données personnelles avec le secteur pharmaceutique – Express [FR]

Appli alerte attentats : «Il faut que la France respecte les standards internationaux»

	Application Alerte Attentats : «Il faut que la France respecte les standards internationaux»

Alors que le gouvernement propose une application pour les alertes aux attentats, Gaël Musquet, hacker et militant du logiciel libre, presse l'Etat d'adopter la diffusion cellulaire, plus efficace et respectueuse de la vie privée.



Alors que le gouvernement propose une appli pour les alertes aux attentats, Gaël Musquet, hacker et militant du logiciel libre, presse l'Etat d'adopter la diffusion cellulaire, plus efficace et respectueuse de la vie privée.
Le gouvernement a dévoilé mercredi une application, «SAIP» (pour «Système d'alerte et d'information des populations»), permettant d'alerter en direct ses utilisateurs en cas d'attentat à proximité. Une bonne initiative, mais une réponse technologique inappropriée, estime Gaël Musquet, hacker en résidence à la Fonderie, l'Agence numérique publique d'Ile-de-France. Car des normes internationales existent déjà pour transmettre une alerte sur tous les téléphones des populations menacées par un risque, sans qu'elles aient besoin d'installer une application, et en respectant leur vie privée.

Que penser de cette application d'alerte gouvernementale ?
Prévoir un protocole d'alerte aux populations est une bonne initiative, on va dans le bon sens. Nous n'avons pas une grande culture du risque en France, donc toutes les occasions d'en parler sont bonnes à prendre ! Cela permet de faire de la pédagogie, d'informer et de former les populations. Car c'est le manque de préparation qui crée de la panique, et malheureusement, parfois des morts. Et puis franchement, les sirènes d'alerte ne sont comprises par personne, donc il est temps de rafraîchir le système avec un peu de technologie.
Le taux d'équipement en smartphones permet aujourd'hui de toucher un maximum de personnes quand on développe une application sur les deux principales plateformes, iOS et Android. Le gouvernement a eu une démarche d'ouverture, en consultant par exemple Visov, une association de volontaires spécialistes de la gestion d'urgence – ils font de la pédagogie auprès des pompiers, des gendarmes ou de l'Etat, entre autres, sur l'utilisation du Web et des réseaux sociaux en cas de crise. Le développement de SAIP est encore en cours, et il appartient au Service d'information du gouvernement [SIG] de recueillir les premiers retours pour améliorer le service. Il a fait cette application de la manière la plus agile possible, on ne peut pas lui faire de reproche là-dessus.

Mais… ?
Il y a plusieurs problèmes avec cette démarche. D'abord, l'application SAIP s'appuie sur les données internet des smartphones, donc sur les réseaux 3G, 4G et wifi qui sont potentiellement vulnérables. Quand il y a trop de téléphones dans une certaine zone et pas assez de canaux disponibles pour pouvoir router tous les appels, les antennes-relais sont saturées et elles ne peuvent plus répondre. Ça se passe régulièrement dans les événements où il y a foule : pendant les attentats de Boston, au discours d'investiture d'Obama mais aussi le 13 Novembre, il y a eu ce qu'on appelle un Mass Call Event (MCE). C'est aussi le cas localement dans des quartiers à cause de concerts, festivals… Quand on sait à l'avance qu'il y aura trop d'appels durant un événement, on installe des antennes-relais supplémentaires pour couvrir le risque de saturation. C'est ce qui va se passer pour l'Euro de foot. Mais en cas de crise imprévue, les infrastructures ne résisteront pas, ni pour les appels, ni pour les SMS, ni pour les données internet. Ce sont des lois physiques, on ne peut rien y faire. Dans ce genre de situation, SAIP sera dans les choux.
Ensuite, il faut faire attention à ne pas morceler le système d'alerte avec de multiples applications de gestion de crise. Il existe une appli pour le risque d'attentats en France, une pour les séismes du Centre sismologique euroméditerranéen, une autre pour mes vacances en Russie et une pour les alertes de l'Indre-et-Loire… Il y a aussi des entreprises privées qui développent leurs propres applications d'alerte, et des fois, comme pour les risques d'avalanches, elles sont meilleures que celles de l'Etat. La concurrence entre les acteurs est contre-productive pour toucher un maximum de personnes. Il vaut mieux un système universel qui puisse aussi s'adresser, par ailleurs, aux touristes de passage en France.
Enfin, il y a la question du respect de la vie privée. Beaucoup d'internautes s'inquiètent déjà, sur Twitter, que l'Etat puisse savoir en permanence où je me trouve via les données de géolocalisation récoltées par cette application. Et il existe effectivement un risque que ces données soient piratées, quels que soient les efforts de sécurisation. Et puis, comme ce n'est pas un logiciel libre, on ne connaît pas son code source et la communauté des développeurs ne peut pas aider à corriger les bugs, faire des stress tests pour vérifier son fonctionnement dans des conditions d'usage intense…

Y a-t-il une meilleure solution ?
A court terme, c'est bien d'avoir une application d'alerte. Mais à long terme, on n'y coupera pas : il faut que la France respecte les standards internationaux de la diffusion cellulaire – cell broadcast en anglais. C'est une norme qui existe déjà pour la diffusion des alertes, et qui permet d'informer toutes les personnes présentes dans la zone de couverture d'une antenne-relais. On n'a pas besoin de connaître leur numéro de téléphone ni de leur faire installer une application : dans la région prédéfinie, tout le monde sans exception reçoit le SMS, y compris les touristes avec un forfait étranger ! C'est une technologie non intrusive qui respecte la vie privée des citoyens. Elle ne se limite pas aux possesseurs d'iPhone et d'Android, même pas besoin d'avoir un smartphone : l'alerte arrive même sur les petits téléphones. Ça tombe bien : en France, 92 % des personnes de plus de 12 ans ont un téléphone, mais 58 % seulement ont un smartphone. Et puis la norme cell broadcast prévoit que les messages d'alerte passent au-dessus de la mêlée dans le trafic téléphonique.

Simulation d'une alerte en diffusion cellulaire sur Android.

La norme du cell broadcast est définie depuis 1995 (pdf et pdf). Elle a même été testée à Paris en 1997 : tout est déjà là ! Depuis, elle a évolué pour supporter les alertes enlèvement (Amber), les séismes et les tsunamis (système ETWS). Avec l'arrivée de la 4G, le protocole a encore été étendu et on peut même l'utiliser pour diffuser des vidéos, aujourd'hui. Vingt ans plus tard, la diffusion cellulaire a été déployée par nos voisins – Espagne, Portugal, Italie, Finlande, Pays-Bas, Chine, Etats-Unis, Israël… Et la France brille par son absence.
Nous devons, nous aussi, la mettre en place dans le cadre d'une véritable politique numérique de l'alerte. Il y a là un enjeu de sécurité publique. Cette norme doit être imposée à nos opérateurs téléphoniques, comme un service public de l'alerte, comme on a imposé la mise en place du 112. C'est une question d'intérêt général. Pourquoi ne respectons-nous pas les normes et standards internationaux en matière d'alerte, documentés, ouverts et qui ont fait leurs preuves ?

Pourquoi n'a-t-on pas encore déployé la diffusion cellulaire en France ?
C'est fragile et ça coûte cher, nous dit-on. Oui, ça coûte cher, mais pas plus que la Hadopi ! On a su débloquer des budgets pour les lobbys de l'industrie culturelle et créer, entretenir, maintenir l'Hadopi à grands frais en contraignant les opérateurs à suivre. Idem pour l'espionnage de masse avec les lois sur la surveillance. Si tu es capable de m'espionner, alors tu es capable de m'informer en cas de crise. Est-ce que notre sécurité vaut moins que les doléances d'autres lobbys ? Nos vies sont-elles moins chères que la Hadopi ?
La mise en place du cell broadcast demande effectivement, quoique pas obligatoirement, de légiférer. Ça demande ensuite que les systèmes d'information des préfectures soient reliés aux systèmes d'information des opérateurs téléphoniques : il faut des passerelles pour que l'alerte passe de la préfecture à SFR, Bouygues et compagnie. Ça demande de la réflexion et un chantier technique. A part ça, c'est simple : les antennes-relais respectent déjà la norme.

Simulation d'une alerte en diffusion cellulaire sur iPhone.

Il faut juste activer l'option. Nos voisins chiliens ont su le faire pour se protéger des tsunamis ; en septembre 2015, il leur a fallu quelques dizaines de minutes seulement pour évacuer des milliers de personnes après le séisme. Il n'y a pas de raison que la France n'y arrive pas aussi !

C'est une question plus générale de culture du risque…
L'alerte est une chose, oui, mais ce n'est pas suffisant. La France est un pays qui fait face à tous les risques possibles, mais nous n'avons pas de culture du risque. Alors que les risques, eux, sont bien là. Notre mémoire est courte mais nous avons des catastrophes naturelles bien plus meurtrières que le terrorisme : 500 morts après la rupture du barrage de Malpasset en 1959, 46 morts avec le séisme provençal de 1909, 29 000 morts pour l'éruption en 1902 de la Montagne Pelée, 70 000 morts dans le tsunami de 1908 à Messine, et même 29 morts récemment à La Faute-sur-Mer et 17 morts dans les inondations de la Côte d'Azur en octobre 2015.
Il faut faire des exercices : un barrage a lâché, que fait-on ensuite ? Les gens paniquent quand ils ne savent pas quoi faire, on l'a encore vu la semaine dernière avec les crues. Il faut des exercices communaux pour expliquer les procédures aux habitants des villes, former des gens à l'utilisation des réseaux sociaux en cas d'urgence pour contrer les rumeurs et diffuser les informations, former des pilotes de drones et des radioamateurs : le jour où il y a un vrai black-out de téléphonie, qui saura faire la transmission des informations ? Au-delà d'événements très médiatiques comme les hackathons ou les simulations entre experts, nous devons impliquer la société civile dans des exercices réguliers.
Commençons à expérimenter sur des territoires français de petite taille, en proie à des crises cycliques – Guadeloupe, Martinique, Réunion, Polynésie… Des formats d'événements existent déjà. CaribeWave, IndianWave et PacificWave sont par exemple des exercices annuels d'alerte au tsunami, auxquels je participe. Les Etats-Unis organisent un «préparathon» contre les catastrophes naturelles.

2016 est l'année de la présidence française de l'Open Governement Partnership. Pour un gouvernement ouvert, à nous, société civile, de nous prendre en charge, nous investir dans les exercices et les réflexions pour une meilleure information et une meilleure préparation aux crises.
Vendredi après-midi, tout le matériel technologique ayant servi à CaribeWaveFWI, la dernière simulation d'alerte au tsunami, sera exposé à la Gaîté Lyrique à Paris, dans le cadre du festival Futurs en Seine.

Article original de Camille Gévaudan

Réagissez à cet article

Original de l’article mis en page : Appli alerte attentats : «Il faut que la France respecte les standards internationaux» – Libération

---

Code de la communication – La loi contre la cybercriminalité à réviser

	Code de la communication – La loi contre la cybercriminalité à révise

---

Les internautes et les utilisateurs des réseaux sociaux espèrent que le projet de code de la communication a abrogé l'article 20 de la loi sur la lutte contre la cybercriminalité. Le gouvernement tiendra-t-il une promesse faite en 2014 ?

Le gouvernement tiendra-t-il les promesses faites par ses anciens membres ? La révision, voire l'abrogation de l'article 20 de la loi sur la lutte contre la cybercriminalité, fait partie des dispositions les plus attendues du projet de code de la communication. Adopté jeudi en conseil des ministres, et attendu incessamment devant les bureaux du Parlement, le projet reste, pour l'instant, inaccessible. Le sort de l'article 20 de la loi contre la cybercriminalité qui avait été abrogé dans l'avant-projet de texte soumis au gouvernement demeure encore inconnu.

Le président de la République ayant déjà affiché sa volonté de supprimer les peines de prison pour sanctionner certains délits de presse comme les injures ou la diffamation, on voit mal comment le Conseil des ministres aurait pu enlever du projet la disposition finale qui a indiqué, entre autres, l'abrogation du fameux article 20. Sanctionnant de peine de prison pouvant aller jusqu'à cinq ans, et d'amende pouvant s'élever jusqu'à 100 millions d'Ariary, toute personne coupable d'injures, de diffamation ou d'atteinte à la dignité d'une personne, par le biais de tout type de support, écrit, audio-visuel ou électronique, le fameux article 20 a soulevé un tollé aussi bien dans le milieu de la presse que parmi les utilisateurs des réseaux sociaux.

La ministre de la Justice et celui de la Communication de l'époque, pour calmer les esprits, avaient alors promis que des ajustements pourraient être apportés au texte s'il devait se trouver en contradiction avec le code de la Communication qui était alors en cours d'élaboration.

Or, en instituant les peines de prison et les amendes exorbitantes pour toute diffamation ou injure faite par voie électronique, la loi, sur la lutte contre la cybercriminalité est entrée en contradiction avec l'esprit qui avait guidé l'élaboration du Code de la communication.

Risque de maintien

De l'eau a, pourtant, coulé sous le pont depuis la validation du texte par le monde médiatique. Vu les relations de la présidence avec les internautes, notamment les utilisateurs du réseau social Facebook, il n'est pas impossible que les autorités aient préféré laisser tel quel l'article 20 de la loi sur la lutte contre la cybercriminalité. L'objectif étant que, comme l'aiment le dire les responsables de la communication des autorités, « limiter le confort de l'internaute qui se trouve devant son clavier et qui se croit intouchable ».

Certaines sources laissent par ailleurs entendre que durant ce long intervalle de temps entre la validation de l'avant-projet et son adoption en conseil des ministres, l'Exécutif a trouvé le temps de réintégrer les dispositions qui avaient été jugées liberticides par les professionnels des médias, et de retirer les articles plus « libéraux », tel que celui qui a abrogé l'article 20 de la loi contre la cybercriminalité. Il semblerait même que le texte, dans une de ses versions manipulées par le Gouvernement, fasse référence à cet article 20 en indiquant que certaines peines seront appliquées sans préjudice de celles prévues par la loi sur la lutte contre la cybercriminalité.

Attendue depuis sa promulgation en 2014, la révision de la loi sur la lutte contre la cybercriminalité, notamment en ce qui concerne l'abrogation de son article 20, pourrait finalement être une réalité maintenant que le code de la communication est en passe d'être adopté. Tout comme la fameuse loi peut encore rester telle une épée de Damoclès suspendue au-dessus de la tête des professionnels des médias, mais aussi des internautes et des utilisateurs des réseaux sociaux.

Réagissez à cet article

Original de l’article mis en page : Code de la communication – La loi contre la cybercriminalité à réviser | LExpress de Madagascar – Actualités en direct sur Madagascar

---

Cloud souverain : les collectivités locales ne pourront pas y couper

Cloud souverain : les collectivités locales ne pourront pas y couper

---

Dans une circulaire publiée au Journal Officiel, le Ministère de la Culture indique que les collectivités locales françaises devront passer par des prestataires hébergés en France pour traiter les données relatives aux citoyens français.

Mieux vaut tard que jamais : une circulaire parue au Journal officiel et signée par la direction générale des collectivités locales et le service interministériel des Archives de France vient clarifier les dispositions relatives au « cloud souverain ». Le texte, repérée par NextInpact, explique que les collectivités françaises devront impérativement passer par des prestataires situés sur le territoire français pour stocker et traiter les données dans le cloud.

Le texte se veut une clarification des directives données dans le cadre du « Guide sur le cloud computing et les datacenters à l'attention des collectivités locales. » La circulaire précise notamment le statut des données produites par les collectivités territoriales. Celles-ci « relèvent du régime politique des archives publiques dès leur création. ».

Point de salut

Outre cet aspect, la circulaire précise quelques lignes plus loin que « toutes les archives publiques sont par ailleurs des trésors nationaux en raison en raison de l'intérêt historique qu'elles présentent ou sont susceptibles de présenter. » Un régime qui s'applique autant aux documents physiques qu'à leurs équivalents numériques et qui implique une nécessaire localisation des données sur le territoire national. Celle-ci ne peut être contournée qu'à titre temporaire sur une demande adressée directement au ministère de la Culture.

Hors des fournisseurs de cloud souverain, point de salut pour les collectivités qui souhaitent avoir recours à ce type de service. La circulaire donne également une définition de ce que l'administration entend par cloud « souverain » : un « cloud dont les données sont entièrement stockées et traitées sur le territoire français. » La circulaire précise également que l'Anssi travaille sur la production d'une offre de labellisation des offres qui répondent à ces critères, label baptisé « Secure Cloud ».

Initié en 2014, le label n'est pas encore entièrement opérationnel et est encore en « phase d'expérimentation » jusqu'à la moitié de l'année 2016 selon le site de l'Afnor. Celui-ci devrait donc sous peu être en mesure de proposer une liste de fournisseurs qualifiés pour répondre aux besoins des collectivités locales en matière de services cloud.

Article original de ZDNet

Réagissez à cet article

Original de l’article mis en page : Cloud souverain : les collectivités locales ne pourront pas y couper – ZDNet

---

L’État crée encore un nouveau fichier secret de données personnelles

L’État crée encore un nouveau fichier secret de données personnelles

---

Le gouvernement a fait connaître vendredi la création d'un fichier de données personnelles utilisé pour les services de renseignement intitulé « #BCR-DNRED », dont le contenu et la portée sont confidentiels. Il s'agit d'un fichier permettant les enquêtes contre la fraude douanière, orienté vers les crimes graves.

Le gouvernement a fait publier vendredi au Journal Officiel un décret n° 2016-725 du 1er juin 2016 qui ajoute un 13e fichier à la liste des fichiers confidentiels de données personnelles mis en œuvre par l'État, « *intéressant la sûreté de l'Etat, la défense ou la sécurité publique* ».
Comme le veut la règle, on ne sait strictement rien de ce fichier si ce n'est qu'il est baptisé « BCR-DNRED » et sera utilisé par les « *services du ministère des finances et des comptes publics (administration des douanes et droits indirects) traitant de la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la prolifération des armes de destruction massive* ».
L'acronyme BCR-DNRED est sans aucun doute une référence à la Direction nationale du renseignement et des enquêtes douanières (DNRED), rattachée à Bercy. Considérée comme un service de renseignement, elle est chargée notamment de collecter des informations sur les les grands trafics de contrebande, et de lutter contre les flux financiers clandestins.

UN FICHIER CONTRE LE TRAFIC

JORF n°0128 du 3 juin 2016
texte n° 87

Délibération n° 2016-010 du 21 janvier 2016 portant avis sur un projet de décret portant création au profit de la direction nationale du renseignement et des enquêtes douanières d'un traitement automatisé de données à caractère personnel dénommé « BCR-DNRED »

NOR: CNIX1614799X
ELI: Non disponible

Avis favorable avec réserve.

L'avis « favorable avec réserve » de la Cnil.

On imagine donc que le fichier BCR-DNRED s'inscrit dans une politique de croisement d'informations concernant de possibles trafics internationaux illicites de biens ou d'argent qui transitent par la France, avec une orientation plus spécifique vers la recherche de financements de crimes graves.
La Cnil, qui n'a pas le droit de publier son avis, a émis un avis « favorable avec réserve », ce qui veut dire qu'elle a estimé qu'au moins sur certains points, le fichier projeté n'était pas conforme à la loi de 1978 sur la protection des données personnelles. Elle avait déjà émis des réserves non publiées concernant les deux derniers fichiers créés par l'État, le fichier CAR relatif au suivi des prisonniers créé en novembre 2015, et le Fichier de traitement des Signalés pour la Prévention et la Radicalisation à caractère Terroriste (FSPRT) modifié quelques jours plus tôt.

Article original de Guillaume Champeau

Original de l'article mis en page : L'État crée encore un nouveau fichier secret de données personnelles — Politique — Numerama

Pour prévenir les violences, un sénateur veut un fichier des interdits de manifester

Pour prévenir les violences, un sénateur veut un fichier des interdits de manifester

Les débordements lors des manifestations organisées chaque semaine contre le projet de loi Travail ont fait réagir Bruno Retailleau. Le sénateur LR vient de déposer une proposition de loi pour instituer notamment un nouveau fichier, celui des interdits de manifester.

Manifester paisiblement, oui, dans la violence, non. Tel est l'angle du texte déposé la semaine dernière par le parlementaire de l'opposition. Son auteur réprouve le fait que désormais, « *les forces de l'ordre sont, de façon répétée, prises pour cible à l'occasion de ces rassemblements* ». Et selon lui, « *un palier dans l'expression de la violence a été franchi, le 18 mai dernier, au cours d'une manifestation interdite lors de laquelle deux fonctionnaires de police ont été lâchement pris à partie et violemment agressés* ».

Dirigée contre les « *casseurs* », dixit son introduction, cette PPL s'inspire du mécanisme existant à l'encontre des hooligans. Le premier article veut ainsi permettre aux préfets de prononcer une mesure d'interdiction de manifester à l'encontre de toute personne « *ayant pris une part active dans un précédent attroupement en cherchant à entraver, par la force ou la violence, l'action des pouvoirs publics* » ou « *impliquée dans la commission d'un acte de dégradation ou de violence à l'occasion de l'une de ces manifestations* ». L'arrêté s'étendrait jusqu'à 12 ou 24 mois selon le comportement de la personne.

Un fichier des interdits de manifester

Pour épauler l'interdiction, qui doit être validée par un vote de l'Assemblée nationale et du Sénat, un traitement automatisé serait nourri de ces arrêtés d'interdiction, mais aussi des noms des personnes condamnées à la peine d'interdiction de participer à des manifestations sur la voie publique (L. 211-13 Code de la sécurité intérieure).

Après passage par la CNIL, sa finalité serait « *de prévenir les troubles à l'ordre public, les atteintes à la sécurité des personnes et des biens ainsi que les infractions susceptibles d'être commises à l'occasion des manifestations sur la voie publique et des rassemblements en lien avec ces manifestations se tenant dans le ressort de leur département* ».

Accentuation du périmètre de la « vidéoprotection »

Le n'est pas tout. L'article 3 vient modifier le régime de la « vidéoprotection ». À ce jour, le Code de la sécurité intérieure autorise « la transmission et l'enregistrement d'images prises sur la voie publique » lorsqu'il s'agit d'assurer « la protection des bâtiments et installations publics et de leurs abords », « la sauvegarde des installations utiles à la défense nationale », « la constatation des infractions aux règles de la circulation », la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés, ou encore la prévention d'actes de terrorisme.

La proposition de loi aimerait ajouter au long inventaire, « *la prévention des troubles à l'ordre public en cas de manifestation sur la voie publique, au besoin au moyen de dispositifs mobiles* ». Pourquoi ? Selon le parlementaire, « *visionner la voie publique ou un lieu ouvert au public n'est possible que dans des cas et pour des motifs définis par la loi. [Cet article] rend possible la mise en œuvre d'un système de vidéo-protection sur le parcours et aux abords immédiats d'une manifestation. Afin d'assurer la faisabilité technique du dispositif, il est prévu de recourir à des caméras mobiles. L'arrêté d'autorisation déterminera la position de chacune des caméras et la période de temps au cours de laquelle le dispositif pourra être utilisé.* »

« Des objets susceptibles de constituer une arme »

La PPL s'intéresse tout autant au Code pénal, et spécialement à l'article concernant la participation délictueuse à une manifestation. Aujourd'hui, il punit de trois ans de prison de prison et 45 000 euros d'amende le fait d'y prendre part en étant porteur d'une arme.

Pour mieux assurer la préservation de l'ordre public, Bruno Retailleau y ajoute le fait « *d'introduire, de détenir ou de faire usage de fusées ou artifices de toute nature ou d'introduire sans motif légitime tous objets susceptibles de constituer une arme* » et celui « *de jeter un projectile présentant un danger pour la sécurité des personnes dans une manifestation sur la voie publique*», sachant que « la tentative de ces délits [sera] punie des mêmes peines ».

Toujours dans cette optique, elle rêve également d'instaurer une prune de 3 750 euros pour quiconque aura introduit ou consommé de l'alcool dans une manifestation sur la voie publique ou participé à une telle réunion « *en état d'ivresse* ».

Provocation à la haine contre les policiers

Outre un élargissement des possibilités d'interdire une personne à participer à des réunions et une obligation de pointage pour les personnes condamnées par un tribunal, la loi de 1881 sur la presse profite également d'une mise à jour. L'idée ? Ériger en infraction le fait de provoquer à la discrimination, à la haine ou à la violence à l'égard d'une personne « *à raison de sa profession* » (jusqu'à un an d'emprisonnement ou/et de 45 000 euros d'amende).

Pour le cas présent, la profession visée est évidemment celle des gendarmes et des policiers. Seront donc concernés ceux qui auront incité, notamment sur Internet, à la haine à l'égard des forces de l'ordre. Le dernier article prévoit d'ailleurs d'instaurer une période de sûreté pour les auteurs de violences contre elles.

S'assembler oui, mais « paisiblement »

Pour justifier son texte, Retailleau se souvient que « *l'article 7 de la Déclaration des droits de l'homme et du citoyen consacre 'le droit de s'assembler paisiblement'* ». Dans le texte fondateur, le principe est plutôt inscrit à l'article 10 (« *Nul ne doit être inquiété pour ses opinions, même religieuses, pourvu que leur manifestation ne trouble pas l'ordre public établi par la Loi* »).

Les adversaires d'un tel dispositif se rappelleront que la Déclaration de 1789 prévoit aussi que « *la Loi ne doit établir que des peines strictement et évidemment nécessaires* » (article 8) sachant que quiconque a le droit de résister à l'oppression (article 2) et que « *la garantie des droits de l'Homme et du Citoyen nécessite une force publique : cette force est donc instituée pour l'avantage de tous, et non pour l'utilité particulière de ceux auxquels elle est confiée* » (article 12).

Merci à Marc Rees, auteur de cet article

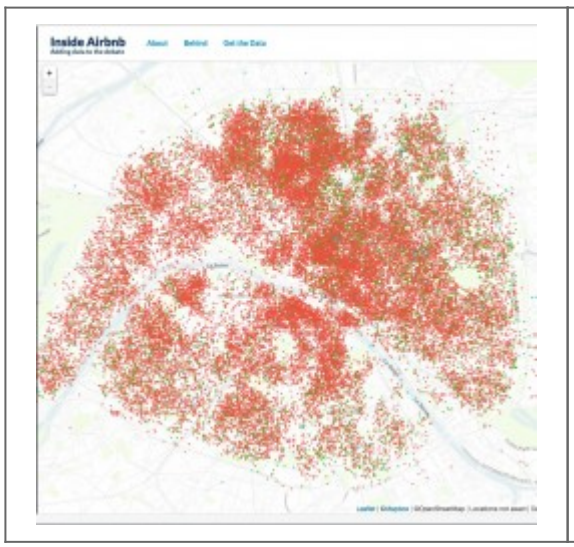
Source : *Pour prévenir les violences, un sénateur veut un fichier des interdits de manifester – Next INpact*

Google fait semblant de ne rien comprendre à ce qu'exige la Cnil

Google fait semblant de ne rien comprendre à ce qu'exige la Cnil

Source : *Droit à l’oubli : Comment Google feint de ne rien comprendre à ce qu’exige la Cnil – Politique – Numerama*

Dénoncez les hôtes Airbnb, Paris vous le rendra…



Dénoncez les hôtes Airbnb, Paris vous le rendra…

La mairie de Paris appelle les voisins à dénoncer les hôtes Airbnb non déclarés aux services municipaux.

Dans le dernier chapitre d'une bataille en cours sur l'économie de partage en France, la ville de Paris demande aux résidents de dénoncer leurs voisins qui ne sont pas correctement enregistrés comme meublé ou hôte du site Airbnb.
Selon le site Europe1.fr, les services municipaux ont créée une nouvelle section sur le portail open data de la ville qui répertorie les résidents qui se sont inscrits comme un hôte Airbnb. 126 résidences sont aujourd'hui listées comme locations saisonnières sur la plate-forme Airbnb alors que le site revendique plus de 41 000 logements (35 185 appartements et 5 827 chambres). Paris serait une des destinations les plus populaires sur sa plate-forme selon Airbnb. Et avec la carte publiée par la ville de Paris, il est facile de repérer les hôtes en règle, c'est à dire qui auront déclarés ces revenus et encaissés la taxe de séjour reversée ensuite à la mairie. C'est une des batailles engagées depuis plusieurs mois par les hôteliers qui crient à la concurrence déloyale. La ville de Berlin a également engagé un bras de fer avec Airbnb pour limiter les locations de meublés sur la plate-forme.

Dans une interview avec Europe1, Mathias Vicherat, chef de cabinet pour le maire de la ville, indique espérer que les résidents utiliseront les informations sur le portail de données ouvertes pour faire pression sur leurs voisins qui ne respectent pas les règles. Les hôtes Airbnb en violation avec les règlements de la ville pourraient faire face à une amende de 25 000€ s'ils louent plus de quatre mois par an leurs logements à des touristes. « On souhaite que cela provoque un espèce de choc de conscience de civisme, et que les gens se mettent en règle d'eux-mêmes, sans attendre d'être éventuellement signalé par un de leurs voisins », dit-il. La mairie explique qu'il n'est pas question d'appeler à la dénonciation comme durant la Seconde Guerre Mondiale où cinq millions de lettres anonymes avaient été envoyées à la police ou la Gestapo… [Lire la suite]

Réagissez à cet article
Article de Serge Leblal

Source : *Paris incite ses habitants à dénoncer les hôtes Airbnb – Le Monde Informatique*