Publier un selfie devant la pyramide du Louvre, est-ce du vol ?

Publier un selfie devant la pyramide du Louvre, est-ce du vol ?

Oui, selon les sénateurs, qui ont réservé cette publication aux particuliers sur des sites strictement non commerciaux pour protéger les droits des créateurs.

Avez-vous le droit de photographier la pyramide du Louvre, et d'en publier l'image sur les réseaux sociaux ? Avez-vous le droit de vous prendre en photo devant la tour Eiffel illuminée en arrière-plan, et de diffuser le cliché ? C'était tout l'enjeu de la « liberté de panorama » qui était soumise à la discussion parlementaire dans le cadre du vote de la loi numérique. Et comme les députés avant eux, les sénateurs ont répondu non. Sauf à demander son avis à l'ayant-droit de l'oeuvre, il sera possible de diffuser des photos de bâtiments ou de sculptures protégées par le droit d'auteur, mais en les réservant aux seuls particuliers et à l'exclusion de tout usage à caractère directement ou indirectement commercial. Excluant de ce champ les associations, les sénateurs ont plongé Wikimedia (l'association qui a pour objet la diffusion de connaissance, via Wikipedia entre autres) dans un cauchemar sans fin : le site internet ne pourra désormais plus illustrer ses articles avec des photos des œuvres dont il parle.

Protéger la démarche artistique

L'objectif de cet amendement est d'empêcher un quidam de tirer un bénéfice financier de l'utilisation d'une photo d'une œuvre (même si c'est lui qui l'a prise) sans en avoir demandé l'autorisation aux ayants-droit de leur créateur, de manière à protéger la création. L'amendement concerne « les reproductions et représentations d'oeuvres architecturales et de sculptures, placées en permanence sur la voie publique », comme par exemple les illuminations de la tour Eiffel ou encore la pyramide du Louvre.

Mais les partisans d'une liberté totale de panorama pointent les restrictions considérables qu'apporte cet amendement. En effet, de tels clichés devenant interdits pour « tout usage à caractère directement ou indirectement commercial », ils seront désormais interdits de séjour sur les réseaux sociaux comme Facebook, Twitter ou Instagram. Il ne restera plus qu'à patienter jusqu'à ce que les œuvres tombent dans le domaine public (70 ans après la mort de l'artiste) pour partager entre amis un selfie touristique, ou bien créer un site internet personnel ne laissant aucune place à la publicité. Le nain de jardin d'Amélie Poulain, photographié devant les monuments du monde entier pour les besoins d'un film – commercial –, ne connaîtrait plus aujourd'hui le même fabuleux destin…. [Lire la suite]

Réagissez à cet article

Source : *Liberté de panorama : publier un selfie devant la pyramide du Louvre, est-ce du vol ?*

Comparateurs de prix : des

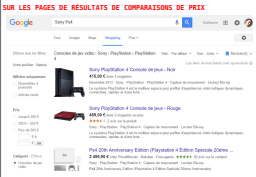
obligations de transparence à partir du 1er juillet

Comparateurs de prix : des obligations de transparence à partir du 1er juillet

À compter du 1er juillet 2016, tous les comparateurs de prix sur internet devront s'astreindre à respecter un certain nombre de règles de transparence.

Le gouvernement a fait publier ce lundi au Journal Officiel un décret n° 2016-505 du 22 avril 2016 relatif aux obligations d'information sur les sites comparateurs en ligne, qui vient mettre en application une disposition de la loi Hamon. Cette dernière avait créé en 2014 un article L115-5 du code de la consommation, qui dispose que « toute personne dont l'activité consiste en la fourniture d'informations en ligne permettant la comparaison des prix et des caractéristiques de biens et de services proposés par des professionnels est tenue d'apporter une information loyale, claire et transparente, y compris sur ce qui relève de la publicité au sens de l'article 20 de la même loi ».

SUR LES PAGES DE RÉSULTATS DE COMPARAISONS DE PRIX



Le décret reprend l'essentiel de ce qui était déjà dans les codes de bonnes pratiques des comparateurs de prix, et qui devient désormais obligatoire. Ainsi à compter du 1er juillet 2016, tous les comparateurs de prix auront l'obligation d'afficher en haut de chaque page de résultats, avant la liste des prix :

1° Le critère de classement des offres utilisé par défaut ainsi que la définition de ce critère, sauf si le critère de classement utilisé par défaut est le prix. La définition est indiquée, à proximité du critère, par tout moyen approprié ;
2° Le caractère exhaustif ou non des offres de biens ou de services comparées et du nombre de sites ou d'entreprises référencés ;
3° Le caractère payant ou non du référencement.

Ils devront aussi informer les consommateurs sur les caractéristiques essentielles des biens ou services comparés, le prix total à payer par le consommateur, et les garanties commerciales offertes.
Si un marchand rémunère le comparateur de prix pour être placé plus haut dans les résultats que ce qu'il serait naturellement, le terme « Annonces » devra figurer sur la page, pour être conforme à l'article 20 de la loi pour la confiance dans l'économie numérique, qui impose d'indiquer comme telles les publicités.

SUR LE SITE INTERNET DU COMPARATEUR DE PRIX
En outre, les comparateurs devront aussi préciser leur mode de fonctionnement « dans une rubrique spécifique », « aisément accessible sur toutes les pages du site et matérialisée par une mention ou un signe distinctif ».

Ils devront au minimum préciser :
1° Les différents critères de classement des offres de biens et de services ainsi que leur définition ;
2° L'existence ou non d'une relation contractuelle ou de liens capitalistiques entre le site de comparaison et les professionnels référencés ;
3° L'existence ou non d'une rémunération du site par les professionnels référencés et, le cas échéant, l'impact de celle-ci sur le classement des offres ;
4° Le détail des éléments constitutifs du prix et la possibilité que des frais supplémentaires y soient ajoutés ;
5° Le cas échéant, la variation des garanties commerciales selon les produits comparés ;
6° Le caractère exhaustif ou non des offres de biens ou de services comparées et du nombre de sites ou d'entreprises référencés ;
7° La périodicité et la méthode d'actualisation des offres comparées.
Notez que pour une raison qui nous échappe, le décret fait systématiquement référence à l'article L111-6 du code de la consommation, relatif aux obligations générales d'information précontractuelles, plutôt qu'à l'article L111-5 qui vise plus spécifiquement les comparateurs de prix… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Suivez nous sur

Réagissez à cet article

Source : *Comparateurs de prix : des obligations de transparence à partir du 1er juillet*

Peut-on s'attendre à la fin de la loi Hadopi ?

Peut-on s'attendre à la fin de la loi Hadopi ?

Les députés ont adopté un amendement qui supprimera l'institution Hadopi en 2022, mais même s'il est promulgué en l'état, le texte ne fait pas disparaître la riposte graduée, qui pourra être reprise par une autre administration.

Il ne faut pas confondre l'Hadopi et la loi Hadopi

Victimes d'un excès d'optimisme, certains imaginent que la riposte graduée elle-même disparaîtra en 2022. Mais il n'en est rien. Si les quatre députés qui ont fait majorité ont bien voté une mise à mort de l'institution Hadopi, il n'en va pas de même pour la riposte graduée.

Plusieurs raisons invitent donc à ne pas sauter trop vite aux conclusions :

Sur l'ensemble des quatre sous-sections du code de la propriété intellectuelle dédiées à la riposte graduée, seule la première intitulée « Compétences, composition et organisation » sera supprimée le 4 février 2022. Les autres, notamment la troisième relative à la riposte graduée, est conservée.

Il sera donc facile pour le législateur de pérenniser la riposte graduée en confiant simplement la riposte graduée à une autre autorité administrative. Comme nous l'expliquions hier, c'est ce qui est proposé dans le rapport Warsmann qui accompagne la proposition de loi examiné par les députés, sur les autorités publiques ou administratives indépendantes : « les compétences (de l'Hadopi) pourraient être transférées soit au CSA, soit à l'ARCEP, soit à une nouvelle AAI ayant une compétence élargie en ces matières ».

Avant cela, le Sénat pourra faire sauter la disposition lorsqu'il examinera lui-même la proposition de loi. Lui qui et traditionnellement attaché à la protection des droits d'auteur devrait y être sensible, même s'il ne sera sans doute pas fâché de se débarrasser d'une patate chaude à quelques mois de la campagne présidentielle.

Enfin, quand bien même le texte serait-il adopté et promulgué, il restera cinq ans à la prochaine majorité, pour glisser dans un projet de loi un amendement qui supprimera l'article qui supprime l'Hadopi. Une seule ligne suffira.

Pour toutes ces raisons, aucun cri d'orfraie n'a été entendu ce vendredi du côté des ayants droit, d'habitude très prompts à publier des communiqués rageurs dès que leurs intérêts sont bousculés. Ils savent que l'affaire est plus anecdotique qu'autre chose, et que le bug législatif sera vite réparé. Voire, que l'amendement adopté leur rend service, puisqu'il précipitera un éventuel transfert des compétences de l'Hadopi vers le CSA, qu'ils appellent de leurs vœux depuis plusieurs années… [Lire la suite]

Réagissez à cet article

Source : *Non, la loi Hadopi ne va pas mourir – Tech – Numerama*

Un piratage sur Tor par le FBI prive les victimes d'une justice

Un piratage sur Tor par le FBI prive les victimes d'une justice

---

La lutte contre la pédocriminalité est une absolue nécessité, qui exige une absolue rigueur. Un juge américain a dû invalider un mandat utilisé par le FBI pour pirater les ordinateurs de membres d'un site pédopornographique hébergé derrière le réseau Tor, privant les victimes et leurs proches de la possibilité d'un procès.

C'est un coup très dur pour le FBI, mais surtout pour les familles des victimes. Dans un jugement prononcé mercredi, un tribunal américain situé au Massachusetts a invalidé le mandat que la police fédérale avait utilisé pour maintenir un site pédopornographique en ligne et procéder au piratage des ordinateurs de plus d'un millier de ses membres. Le site en question, Playpen, n'était accessible qu'à travers le célèbre réseau d'anonymisation Tor, qui masquait l'adresse IP véritable des visiteurs, rendant très difficile leur identification et leur poursuite.
C'est sur un argument purement juridictionnel que s'est appuyé le magistrat pour dénoncer l'illégalité du mandat employé par le FBI. Selon le code de procédure pénal américain, les magistrats n'ont pas l'autorité suffisante pour émettre des mandats situés en dehors de leur compétence géographique. C'est pourtant ce qu'il s'est produit dans au moins l'un des cas de l'affaire Playpen.
Le site The Intercept, qui se fait l'écho des conclusions de la décision, explique en effet que le mandat a été émis au départ par un juge se trouvant en Virginie. Or, l'un des suspects qui a été attrapé par le FBI dans le cadre de l'enquête vit dans le Massachusetts. Les éléments contre lui – qui est à l'origine de la plainte visant à obtenir l'invalidation du mandat – ne peuvent donc pas être retenus comme preuves, car ils ont été obtenus sans mandat valable.
Le verdict rendu cette semaine risque fort de réduire à néant toute la stratégie du FBI pour faire fermer Playpen et mettre la main sur ses visiteurs américains. La décision est tout à fait susceptible de faire tache d'huile. D'autres accusés pourraient très bien se mettre à attaquer la légalité du mandat sur le même argument juridictionnel, ce qui ferait tomber des preuves à charge contre eux.
Christopher Soghoian, membre de l'American Civil Liberties Union, une association de protection des droits et libertés aux États-Unis, indique que le piratage du site pédopornographique a permis de constituer 1 300 dossiers en attente. À supposer que tous vivent aux USA, combien se trouvent dans des États qui sont en dehors de la compétence géographique de la Virginie ? Sans doute une grande majorité.

UNE FAILLE LÉGISLATIVE BIENTÔT CORRIGÉE ?
Cette règle de la procédure pénale pourrait toutefois disparaître. Le département de la justice américain souhaite lever cette barrière afin que les juges puissent délivrer des mandats pour des recherches à distance sur des ordinateurs qui sont situés en dehors de leur juridiction ou lorsque leur emplacement géographique est inconnu.
Selon The Intercept, le changement législatif a de bonnes chances de passer et le feu vert de la Cour Suprême est très probable – il devrait survenir très bientôt – malgré les protestations des organisations de défense des libertés individuelles et de quelques sociétés, comme Google. Le Congrès aura ensuite six mois pour l'approuver ou la rejeter, sinon la modification entrera en vigueur.

L'AFFAIRE PLAYPEN ET LE PIRATAGE DU FBI
L'affaire Playpen remonte début 2015, quand le FBI parvient à prendre le contrôle des serveurs du site. Au lieu de le fermer tout de suite, la police choisit une autre approche, celle du honeypot : le site reste actif pendant environ deux semaines, sur les serveurs du FBI, afin de savoir qui se connecte sur Playpen. Tactique qui provoquera au passage un déluge de critiques sur le FBI.
C'est au cours de cette période que le FBI a procédé à la contamination des ordinateurs des visiteurs, afin de collecter des informations sur eux, comme leur véritable adresse IP, qui est habituellement masquée avec le réseau d'anonymisation. En effet, la connexion transite par une succession de relais afin de camoufler la géolocalisation du PC. C'est avec ces données que le FBI s'est ensuite adressé aux opérateurs pour obtenir l'identité des internautes – en tout cas ceux aux USA… [Lire la suite]

Réagissez à cet article

Source : *Pédopornographie : quand un piratage par le FBI sur Tor prive les victimes d'une justice*

Avant le règlement européen sur les données personnelles, la Loi pour la République Numérique

	Avant le règlement européen sur les données personnelles, la Loi pour la République Numérique

Le nouveau règlement européen relatif à la protection des données personnelles (GDPR) fait grand bruit en Europe. Il donne, en effet, plus de droits aux consommateurs sur la façon dont leurs données sont traitées et requiert des contrôles complémentaires (et des informations) sur quiconque dispose de données personnelles dans l'Union européenne.

Comme toutes les lois, celle-ci a été largement discutée, avec des points de vue contradictoires, mais une chose a été acceptée par tous : les entreprises auront deux ans, à compter de la date de publication de la loi (en juin 2016), avant que celle-ci entre en vigueur. Deux années indispensables aux entreprises pour leur permettre de mettre en place les politiques, les processus et les technologies nécessaires pour être en conformité avec le règlement.
En avance sur ses voisins européens, la France a d'ores et déjà adopté un projet de loi en phase avec les principes fondamentaux du règlement européen relatif à la protection des données personnelles. Ainsi, le projet de loi pour une République numérique, validé par l'Assemblée nationale le 26 janvier dernier (actuellement examiné par le Sénat), devrait être approuvé pour entrer en vigueur cette année.

Quelles sont les grandes lignes de la loi pour la République numérique ?

Droit à la portabilité des données : le consommateur peut demander à ce que ses données soient conservées par le responsable du traitement des données et dispose en toutes circonstances d'un droit de récupération de ses données.
• Conservation des données : le responsable du traitement des données doit informer le consommateur de la durée pendant laquelle les données sont conservées.
• Droit de rectification : les consommateurs peuvent demander à ce que leurs données soient éditées pour les modifier.
• Droit à la suppression : les personnes concernées peuvent demander à ce que leurs données soient supprimées ou interdire l'usage de leurs données.
• Recours collectifs : les consommateurs peuvent déposer une plainte collective pour demander réparation lors de la perte ou de l'utilisation abusive de leurs données.
• Amende maximale : celle-ci peut aller de 150.000 à 20.000.000 euros ou 4 % du chiffre d'affaires global, pour l'amende la plus élevée.
D'autres pays vont-ils prendre exemple sur la France pour faire avancer leurs propres législations sur la protection des données avant la mise en œuvre du règlement européen ? Il y a fort à parier que oui. Et les entreprises ont également anticipé cette nouvelle réglementation puisque l'utilisation de services cloud basés dans la zone européenne a presque doublé en six mois (de 14,3 % au premier trimestre 2015 à 27 % pour 2016)… [Lire la suite]

Réagissez à cet article

Source : *Nouveau règlement européen sur les données personnelles : la France en avance sur ses voisins européens – Global Security Mag Online*

Le hacking légal et rémunéré, vous connaissez ?

Le hacking légal et rémunéré, vous connaissez ?

Le hacking : « accès et maintien frauduleux dans un système de traitement automatisé de données » va changer. Le 21 janvier 2016, l'Assemblée nationale a adopté, en première lecture, un amendement contenu dans le projet de loi pour une République numérique visant à compléter l'article 323-1 du Code pénal, par un nouvel alinéa :

« Toute personne qui a tenté de commettre ou commis le délit prévu au présent article est exempte de peine si elle a immédiatement averti l'autorité administrative ou judiciaire ou le responsable du système de traitement automatisé de données en cause d'un risque d'atteinte aux données ou au fonctionnement du système ».
Cet amendement, nommé « Bluetouff » en référence à l'arrêt de la Cour de cassation du 20 mai 2015 qui avait condamné un internaute pour s'être maintenu frauduleusement dans l'intranet de l'ANSES, prévoit, comme en matière d'association de malfaiteurs, une exemption de peine pour toute personne qui, après avoir constaté, voire exploité, une faille de sécurité en informe immédiatement l'autorité publique ou le maître du système.
Il ne s'agit là que d'une exemption de peine, et non d'une exemption de poursuites, ce qui en d'autres termes signifie que l'auteur du hacking, du piratage pourra être poursuivi et déclaré coupable, mais n'aura pas à exécuter de peines pénales.
Par cet amendement, le Gouvernement entend poursuivre un double objectif. D'abord donner une alternative presque légale au hacker du dimanche qui par défi personnel, et non intention de nuire, est parvenu à s'introduire dans un système d'information. A ce titre, il est regrettable que l'amendement Bluetouff ne prévoit qu'une exemption de peine, l'assurance de ne pas être poursuivi pour hacking aurait, à n'en pas douter, été plus convaincante.
En second lieu, il permettrait de participer à la sécurité du réseau. Garantie en poche de ne pas être pénalisés, nombre d'experts en informatique pourraient collaborer avec les sociétés développant des sites internet, applications ou logiciels pour identifier et corriger les vulnérabilités.
Ce dispositif serait, toutefois, incomplet s'il ne pouvait, par ailleurs, s'appuyer sur des initiatives de plus en plus courantes du secteur privé.
Les grands noms de l'internet et de l'informatique sont de plus en plus nombreux à proposer, souvent contre rémunération, aux hackers bien intentionnés de collaborer avec eux pour détecter les failles de sécurité.
Calqué sur ce qui existe déjà aux Etats-Unis avec la plateforme HackerOne, le site européen Bounty Factory mettant en relation hackers et entreprises du net permet depuis peu, en échange de récompenses pour toute faille décelée et corrigée, de signaler en ligne les vulnérabilités.
Législateur et secteur privé s'acheminent progressivement vers un droit au hacking. En attendant, le Code pénal nous rappelle qu' « accéder ou se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 euros d'amende ».

Virginie Bensoussan-Brulé
Julien Kahn
Lexing Pénal numérique

Réagissez à cet article

Source : *Le hacking ça peut payer… légalement*

Vers un délit d’entrave au blocage des sites faisant l’apologie du terrorisme ?

Vers un délit d’entrave au blocage des sites faisant l’apologie du terrorisme ?

Dans le cadre du projet de loi sur la réforme pénale, le rapporteur Michel Mercier veut instaurer en France un délit d'entrave au blocage des sites « terroristes ».

En préparation de l'examen en Commission des lois, le sénateur a déposé un amendement visant à condamner ceux qui viennent entraver les procédures de blocage des sites faisant l'apologie ou provocant au terrorisme. Celui qui viendrait extraire, reproduire et transmettre intentionnellement les données concernées par ces mesures, « en connaissance de cause », serait ainsi éligible à cinq ans de prison et 75 000 euros d'amende.
Cette mesure, puisée directement dans une proposition de loi sénatoriale contre le terrorisme (UDI/LR), viendra épauler les mesures de blocage administratif de ces sites, permises depuis la loi du 13 novembre 2014 sur le terrorisme, ou celles décidées par un juge en application de l'article 706-23 du code de procédure pénale.
« *Ces blocages, administratif ou judiciaire, ont pour but de lutter contre la diffusion de contenus faisant l'apologie d'actes de terrorisme,* explique l'auteur de l'amendement dans son exposé des motifs. *Néanmoins, ces blocages peuvent être entravés par certains comportements. Ces derniers, s'ils ne consistent pas en la diffusion publique de ces contenus, ne peuvent être appréhendés sous le délit d'apologie d'actes de terrorisme ou de provocation à de tels actes* ».
Cette mesure est rédigée en des termes suffisamment larges pour qu'on puisse imaginer la sanction de celui qui viendrait tweeter ou publier sur Facebook les données litigieuses, puisqu'il n'est pas possible de bloquer l'un ou l'autre de ces réseaux. Remarquons surtout que le texte n'exige pas nécessairement de diffusion publique. Il joue dès lors qu'on extrait, reproduit et transmet ces données d'une manière ou d'une autre, à destination par exemple d'un serveur distant. Du coup, l'amendement est également taillé pour frapper ceux qui multiplient des contre-mesures aux blocages par IP ou DNS… [Lire la suite]

Réagissez à cet article

Source : *Vers un délit d'entrave au blocage des sites faisant l'apologie du terrorisme ? – Next INpact*

Loi sur le numérique adoptée quasiment sans voix contre

#Loi sur le numérique adoptée quasiment sans voix contre

La loi Pour une république numérique » vient d'être adoptée par l'Assemblée Nationale à 356 contre 1. Elle sera prochainement examinée au Sénat pour une seconde lecture.
La loi sur le numérique d'Axelle Lemaire vient d'être adoptée par une majorité de députés de l'Assemblée aujourd'hui. Sur 544 votants, 356 se sont prononcés en faveur de la nouvelle loi obtenant ainsi une large majorité.
Ainsi que la Secrétaire d'Etat chargée du Numérique l'avait énoncé devant l'Assemblée la semaine dernière, la loi est voulue construite selon la devise française, en trois axes :
• circulation des données et du savoir (liberté),
• protection dans la société numérique (égalité),
• l'accès des publics fragiles au numérique (fraternité).

Le gouvernement inscrit donc désormais dans le marbre législatif sa volonté de ne pas rater la vague de l'Open Data (Royaume-Uni, Danemark), tout en fournissant un nouveau cadre aux sites Internet et aux FAI (neutralité, loyauté des plates-formes).
Le vote a aussi permis de révéler que 187 votants se sont abstenus, la plupart des députés du groupe Les Républicains, avouant leur désapprobation de forme, et non de fond, du projet de loi dévoilé pour la première fois au début de l'été 2015.

Réagissez à cet article

Source : *La loi sur le numérique adoptée à 356 voix contre 1*

Amnesty critique la nouvelle loi sur la cybercriminalité au Koweït

	**Amnesty critique la nouvelle loi sur la cybercriminalité au Koweït**

Amnesty International a vivement critiqué mardi une nouvelle loi sur la cybercriminalité au Koweït qui, selon cette organisation, va restreindre davantage la liberté d'expression et doit être révisée.

Le texte, qui entre en vigueur mardi, « va s'ajouter à l'éventail de lois sur le web qui restreignent déjà le droit des Koweïtiens à la liberté d'expression et doit être révisé d'urgence », écrit l'organisation de défense des droits de l'Homme dans un communiqué.
La nouvelle législation prévoit la criminalisation d'une série d'expressions en ligne comportant notamment des critiques envers le gouvernement, des dignitaires religieux ou des dirigeants étrangers, relève Amnesty.
« Cette loi répressive » fait partie d'un éventail de législations destinées à « étouffer la liberté d'expression », a commenté Saïd Boumedouha, directeur adjoint d'Amnesty International pour le Moyen-Orient et l'Afrique du nord.
Des dizaines de personnes au Koweït ont été arrêtées et poursuivies en justice, certaines servant déjà des peines de prison, en vertu d'une autre législation pour des commentaires sur les réseaux sociaux.
Votée en juin, la nouvelle loi prévoit des peines de 10 ans de prison et des amendes allant jusqu'à 165.000 dollars pour des crimes en ligne, notamment ceux liés au terrorisme.
Pour le gouvernement, cette loi est nécessaire pour combler un vide juridique et réglementer l'utilisation des services en ligne tels que Twitter.
La peine minimale en vertu de la loi consiste en six mois de prison et 6.600 dollars d'amende pour celui qui ose, illégalement, « infiltrer un ordinateur ou un réseau électronique ».
« Les autorités koweïtiennes ne doivent pas appliquer cette loi jusqu'à ce qu'elle soit révisée pour se conformer aux obligations internationales du Koweït en matière de droits de l'Homme », a dit M. Boumedouha.
« Cette loi n'appartient pas au XXIe siècle », a-t-il ajouté, soulignant que « les Koweïtiens méritent mieux » qu'une telle législation.

Réagissez à cet article

Source : *Koweït: Amnesty critique la nouvelle loi sur la cybercriminalité – Internet – Notre Temps*

Wi-Fi interdit, Tor bloqué, backdoors… les nouvelles idées au gouvernement

Wi-Fi interdit, Tor bloqué, backdoors… les nouvelles idées au gouvernement

La liste des mesures envisagées par le gouvernement pour renforcer la sécurité au détriment de la liberté et de la vie privée s'allonge. Alors que le gouvernement envisage déjà de nouvelles lois sécuritaires qui permettraient par exemple de croiser tous les fichiers de données personnelles détenues par l'État, d'obliger à l'installation d'émetteurs GPS sur les voitures louées, d'allonger la durée de conservation des données de connexion ou encore de faciliter le recours aux IMSI-catchers, Le Monde révèle samedi de nouvelles mesures recensées par le ministère de l'Intérieur.
Le quotidien a en effet pu consulter un tableau édité en interne le mardi 1er décembre par la direction des libertés publiques et des affaires juridiques (DLPAJ), qui dépend du ministère de l'Intérieur de Bernard Cazeneuve. C'est elle qui prépare les projets de lois et de décrets relatifs aux libertés publiques et à la police administrative. C'est donc dans ce cadre, pour rédiger deux nouveaux textes législatifs – l'un sur l'état d'urgence, l'autre sur l'anti-terrorisme, que la DLPAG a dressé les mesures demandées par la police ou la gendarmerie qui pourraient être inscrites dans les textes attendus pour janvier 2016.

Interdire et bloquer TOR en France
Parmi ces mesures qui ne sont encore que des hypothèses de travail figure une série de nouvelles restrictions aux libertés sur Internet :
« Interdire les connexions Wi-Fi libres et partagées » et fermer toutes les connexions Wi-Fi publiques pendant l'état d'urgence, « sous peine de sanctions pénales ».
Jusqu'à présent la loi impose par principe aux abonnés à internet de sécuriser leur connexion pour éviter qu'elle soit utilisée à des fins illicites, mais le seul risque que prennent les abonnés généreux et récalcitrants qui laissent leur Wi-Fi ouvert est de recevoir un avertissement Hadopi si quelqu'un l'utilise pour pirater des films ou de la musique. En obligeant à fermer toute connexion, la police s'assurerait d'avoir un identifiant précis pour chaque adresse IP, ou au moins de réduire la liste des suspects possibles dans un même foyer. C'est en tout cas l'idée.
« Interdire et bloquer les communications des réseaux TOR en France » : Même à supposer que ça soit techniquement possible, ce serait une mesure totalement disproportionnée qui enverrait un très mauvais signe à l'international, alors que le réseau d'anonymisation TOR est utilisé par de très nombreux activistes et dissidents de pays autoritaires. L'un des premiers pays à avoir bloqué Tor était l'Iran.
« Identifier les applications de VoIP et obliger les éditeurs à communiquer aux forces de sécurité les clefs de chiffrement » : C'est la fameuse grande guerre du chiffrement à laquelle se prépare La Quadrature du Net, la France ayant sans aucun doute la volonté de se joindre à la Grande-Bretagne pour obtenir que les éditeurs de messagerie chiffrée fournissent des backdoors pour que les autorités puissent écouter les conversations interceptées.

Réagissez à cet article
Source : http://www.numerama.com/politique/133795-wi-fi-ouvert-interdit-tor-bloque-les-nouvelles-idees-de-la-police.html