

MAI 2024 - N°501

EXPERTISES DES SYSTÈMES D'INFORMATION

EXPERTISES

DROIT, TECHNOLOGIES & PROSPECTIVES

SAINT-GOBAIN
**UNE GESTION
AGILE DES FLUX
TRANSFRONTALIERS
DE DONNÉES**

GOOGLE CHROME : EFFACEMENT DES DONNÉES DES INTERNAUTES AMÉRICAINS SEULEMENT

Google s'est engagé à détruire les données récoltées sur plus de 136 millions d'internautes américains ayant utilisé le navigateur Google Chrome après avoir activé l'option « navigation privée », selon un projet de règlement de recours collectif rendu public le 1er avril dernier. Cet accord s'inscrit dans une class action initiée en juin 2020 contre Google l'accusant d'avoir induit les internautes en erreur sur

la garantie du caractère privé de la navigation sur Chrome en application de cette option. Google s'est par ailleurs engagé à réécrire « immédiatement » la mention qui s'affiche pour cette option, afin d'*informer les utilisateurs qu'il collecte des données de navigation privée*. De plus, Google a indiqué avoir clarifié de nombreuses informations concernant la collecte de données des utilisateurs et les activités que les sites

web peuvent visualiser pendant que les utilisateurs naviguent en mode « navigation privée ». L'entreprise a également accepté de permettre aux clients de bloquer les cookies tiers pendant cinq ans lorsqu'ils utilisent le mode navigation privée. Le porte-parole de Google a déclaré : « nous sommes heureux de supprimer d'anciennes données techniques qui n'ont jamais été associées à des individus et n'ont jamais été utilisées pour une quelconque forme de personnalisation. » Reste désormais au tribunal de valider cet accord.

Une loi du Colorado protège les données cérébrales

Le 17 avril dernier, le gouverneur du Colorado a signé la première loi qui, aux États-Unis, protège les données personnelles issues du cerveau. Cette nouvelle loi élargit la définition des « données sensibles » dans l'actuelle loi de l'État, le Colorado privacy act, qui inclut déjà les empreintes digitales, les images faciales et autres données biométriques. Cette nouvelle loi protège les données « générées par le traitement technologique, la mesure ou l'analyse des propriétés,

compositions ou activités biologiques, génétiques, biochimiques, physiologiques ou neuronales d'une personne, ou du corps ou des fonctions corporelles d'une personne », explique le site officiel de l'État, « ces données étant utilisées ou destinées à être utilisées, seules ou en combinaison avec d'autres données à caractère personnel, à des fins d'identification. » précise-t-il. Les données neuronales peuvent révéler des informations intimes sur les individus, comme la santé, les états mentaux, les émotions et la fonction cognitive. Ce texte ne s'applique qu'aux technologies cérébrales grand public qui se développent et sont déjà commercialisées mais pas aux données obtenues en milieu clinique.

CYBERSQUATTING : 1ÈRE MISE EN DEMEURE NOTIFIÉE PAR NFT

Contrairement à l'idée reçue, il n'y a pas d'anonymat sur la blockchain. L'affaire Boischaut, du nom de la maison de vente aux enchères Boischaut qui a été victime d'un cybersquatteur, en est la preuve. Boischaut est une des principales maisons de vente opérant des ventes de NFT en France. Un cybersquatteur a réservé boischaut.eth sur la blockchain open source Ethereum et a proposé, via le compte X (Twitter) de la société Boischaut, de lui restituer le nom de domaine boischaut.eth contre rémunération, avant de le mettre en vente sur le marché secondaire. Pour récupérer son nom

de domaine sans céder au chantage, encore fallait-il identifier celui qui le détenait. Comme l'explique Jordan Tarlet, co-fondateur de la société Eneptyts, qui a été chargé de rechercher l'identité du cybersquatteur, « l'anonymat sur la blockchain est un mythe. Toutes les transactions sont transparentes. Et dans cette chaîne de valeur, il y a toujours quelqu'un qui connaît l'identité », notamment au moment de la conversion de cryptomonnaies en monnaies fiduciaires. Dans ce type d'affaires, il explique que la levée de l'anonymat est facilitée par le fait que le cybersquatteur utilise Twitter pour proposer la restitution

du nom de domaine. Comme beaucoup, il a affiché sur Twitter un nom de domaine blockchain. En recherchant toutes les transactions opérées par cet individu via cette adresse, Jordan Tarlet a recherché avec qui il avait interagi, ce qui facilite l'identification de plateformes tierces pouvant détenir son identité. Le cybersquatteur a par la suite été mis en demeure de restituer ce nom de domaine sous peine de poursuites civiles et pénales. L'avocat Matthieu Quiniou a conçu cette mise en demeure NFT, envoyée dans le wallet de l'individu grâce aux smart contracts, sans possibilité pour celui-ci de le supprimer.

Une mission du CSPLA sur l'obligation de transparence de l'IA Act

Le 12 avril dernier, la ministre de la Culture a confié au CSPLA une nouvelle mission relative au règlement sur l'intelligence artificielle qui oblige les fournisseurs de modèles d'IA à usage général de prendre des mesures visant à respecter le droit d'auteur. Les fournisseurs devront en effet élaborer et rendre disponible publiquement un « résumé suffisamment détaillé » des données ayant servi à l'entraînement de leur modèle. Dans sa lettre de mission, Rachida Dati demande que le CSPLA expertise la portée de l'obligation de transparence prévue

par le règlement européen, compte tenu des interrogations et établisse la liste des informations paraissant devoir nécessairement être communiquées, selon les secteurs culturels concernés, pour permettre aux auteurs et aux titulaires de droits voisins d'exercer leurs droits. La mission est confiée à Alexandra Bensamoun, professeure de droit à l'université Paris Saclay, ancienne membre de la Commission de l'intelligence artificielle, avec le concours de Frédéric Pascal, professeur des Universités à CentraleSupélec - Université Paris-Saclay et directeur de l'institut DataIA. Un point d'étape sera présenté à l'été 2024, et les conclusions de ce rapport à la fin de cette année.

USA

PROLONGATION DU FISA

Le 20 avril dernier, le Congrès des États-Unis a voté la prolongation jusqu'en 2026 du Foreign Intelligence Surveillance Act (Fisa) dont la section 702 autorise la NSA

ou le FBI à accéder aux « communications de non-Américains à l'étranger ». Cette loi qui devait expirer le 19 avril 2024 a été prolongée par un vote bipartisan.