CANARD ENCHAINE du 28 janvier 2026

Le gouvernement fait le jeu des pirates pour écouter aux portes

LES CONVERSATIONS sur Signal, Telegram ou WhatsApp sont aujourd'hui chiffrées, ce qui les rend invisibles aux plateformes qui les abritent, comme aux services de renseignement. Une protection qui bénéficie aux citoyens lambda, mais aussi aux grands criminels. Conséquence? Le gouvernement est prêt à tout pour faire sauter ces verrous.

Dans le cadre de la proposition de loi contre le narcotrafic examinée en mars dernier par le Parlement, l'ancien ministre de l'Intérieur Bruno Retailleau et celui de la Justice, Gérald Darmanin, avaient tenté d'imposer des *backdoors* (« portes dérobées », en bon français), un dispositif permettant de casser le chiffrement des discussions privées et de contraindre les messageries cryptées à livrer les discussions de leurs utilisateurs aux enquêteurs. Mais la disposition avait été rejetée tout net par les parlementaires.

Le vieux disque des "backdoors"

Et pour cause… « *Les* backdoors *reviennent à espionner les gens et remettent en cause le droit à la vie privée et à la protection des données,* affirme le sénateur centriste Olivier Cadic. *On est en train de préparer le terrain pour qu'un régime autoritaire s'installe !* » De quoi péter un câble…

Les portes dérobées affaiblissent aussi la sécurité des applications. Si on décodait une partie des conversations, toutes se retrouveraient fragilisées. Dès lors, les failles pourraient être exploitées par les services de renseignement… mais aussi par des groupes criminels et des Etats hostiles contre lesquels ils prétendent justement lutter. Un sacré bug !

Pour s'assurer que les ministres régaliens n'essaient pas de revenir par la fenêtre pour imposer des portes dérobées, Cadic avait introduit dans le projet de loi Résilience contre les cyberattaques un amendement les interdisant formellement, et ce avec le soutien du Premier ministre de l'époque, François Bayrou. Dix mois plus tard, le gouvernement refuse d'inscrire à l'ordre du jour de l'Assemblée ce texte, qui transcrit dans le droit français plusieurs directives européennes visant à prémunir les entreprises et les administrations contre les piratages.

En décembre, Matignon a même demandé au sénateur Cadic de jeter son amendement à la corbeille, ce qu'il a refusé de faire. Pour le court-circuiter, le ministère de l'Intérieur songe désormais à faire voter une loi autorisant les *backdoors* avant l'entrée en vigueur des directives européennes en France.

Il y a pourtant urgence à adopter la loi Résilience : les fuites de données sont quotidiennes, et même Beauvau a subi les attaques des flibustiers. En refusant d'adopter le texte européen – qui aurait dû l'être dès octobre 2024 –, la France est, par ailleurs, menacée d'une amende d'un montant compris entre 30 et 50 millions d'euros, ce que lui a rappelé l'Union européenne dans un récent courrier. Message reçu ?

Prends tes clics et tes hacks

Lecornu continue pourtant de jouer la montre. Le 19 janvier, il a nommé Florent Boudié, le président macroniste de la Commission des lois, à la tête d'une mission destinée à explorer les « *possibilités d'évolution des dispositifs juridiques existants* » concernant l'accès aux communications chiffrées (« Le Monde », 22/1). Ses conclusions sont attendues pour le mois d'avril.

En parallèle, la délégation parlementaire chargée de contrôler l'action du gouvernement en matière de renseignement promet de rendre, au printemps, un rapport sur les messageries cryptées et de déposer un texte favorable au décryptage. Au niveau européen, un groupe de travail sur le chiffrement a été lancé en fin d'année.

« *A ce rythme, quand la France entérinera les directives européennes écrites en 2022, elles seront obsolètes !* » s'inquiète le député Philippe Latombe. Dans un courrier daté du 13 décembre, l'élu Démocrates a prévenu la ministre du Numérique, Anne Le Hénanff, qu'elle pourrait être « *tenue pour responsable* » si une victime de cyberattaque se retournait contre le gouvernement pour « manquement » en matière de sécurisation des systèmes d'information.

Pour avoir tardé à prendre des mesures, l'Etat sera-t-il bientôt condamné à indemniser des milliers d'internautes hackés… à contre-hackeur?

Fanny Ruz-Guindos

Les barbouzes se jettent allô !

POURQUOI réclamer des « portes dérobées » quand la crème des services secrets assure ne pas en avoir besoin? Nicolas Lerner, le patron de la Direction générale de la sécurité extérieure (DGSE), estime que ses gars disposent d'outils maison supérieurs aux *backdoors* (France Inter, 10/11): « *Vous avez un certain nombre de logiciels, de solutions soit commerciales, soit étatiques qui permettent de capter ce qui s'écrit sur les téléphones avant que ce soit chiffré.* »

En clair, les agents de « la Piscine » n'ont pas besoin de demander l'accès à des plateformes peu coopératives puisqu'ils ont directement accès aux mobiles… « *La DGSE a les moyens de faire un double des clés pour surveiller les conversations quand la DGSI* (la Direction générale de la sécurité intérieure), *moins bien armée, aimerait défoncer la porte* », décrypte un expert du renseignement auprès du « Canard ».

Si la DGSI, la Coordination nationale du renseignement et de la lutte contre le terrorisme et le Groupement interministériel de contrôle sont favorables aux portes dérobées, c'est qu'ils sont moins bien outillés que la DGSE? Cet aveu de faiblesse mériterait qu'ils prennent la porte!