À l'attention de:
Ministre de la Justice, Vice-Premier ministre M. Vincent Van Quickenborne
Ministre des Télécommunications, Vice-Premier ministre Mme Petra De Sutter
Ministre de la Défense, Mme Ludivine Dedonder

Le chiffrement de bout-en-bout garantit la sécurité du peuple belge.

Le chiffrement nous protège dans nos activités quotidiennes, telles qu'accéder à son compte bancaire en ligne, sécuriser des données confidentielles comme des fiches de paies ou des informations fiscales, et communiquer avec nos amis et nos familles. Le chiffrement de bout-en-bout protège aussi les communautés vulnérables et les professions pour lesquelles les communications privées sont essentielles, tels que les journalistes, avocats, et professionnels de la santé.

Le gouvernement belge a récemment proposé une nouvelle législation, considérée comme la plus dangereuses parmi les États Membres de l'Union Européenne, qui porte atteinte à la sécurité et la protection de la vie privée offerte par le chiffrement de bout-en-bout.

L'*avant-projet de loi relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités*[1], ou la « *Loi sur la conservation des données* », exige des opérateurs de systèmes chiffrés de permettre aux forces de l'ordre d'accéder, sur demande, au contenu produit par un utilisateur spécifique à compter d'une date déterminée. Ce faisant, il est attendu de ces derniers qu'ils soient capables d'« arrêter » le chiffrement pour des utilisateurs spécifiques. Or, il n'est pas possible de simplement « arrêter » le chiffrement ; en pratique cela signifie que les opérateurs vont devoir créer un nouveau système de fourniture de leurs services et orienter les utilisateurs concernés vers ce nouveau système de fourniture distinct. Non seulement cela nécessite des changements techniques importants, mais cela aura pour effet de rompre la promesse de confidentialité et de protection de la vie privée des services de communications chiffrés de bout-en-bout.

Cette mesure n'améliore à l'évidence pas la sécurité des belges, et au contraire, porte atteinte à l'utilisation du chiffrement de bout-en-bout en Belgique et, comme le précise l'Autorité de Protection des Données belge dans son avis contre la Loi sur la conservation des données, force les entreprises à créer des « de facto backdoor »[2] dans leurs systèmes. Le consensus au sein de la communauté d'experts en cybersécurité est sans appel : il n'est pas possible de donner accès à des communications chiffrées de bout-en-bout à des tiers sans créer des portes dérobées et des vulnérabilités qui peuvent être exploitées par toute personne qui les trouve[3]. En d'autres termes, il n'est pas possible de donner accès aux forces de l'ordre à des portes dérobées, sans prendre le risque de voir des acteurs malintentionnés eux-aussi y avoir accès. Créer des portes dérobées au chiffrement affaiblit la sécurité de l'ensemble du système, et met en danger tous ses utilisateurs[4]. Porter atteinte au chiffrement en introduisant des portes dérobées aux communications chiffrées expose la Belgique à des attaques, y compris contre les journalistes,

[1] https://ibpt.be/index.php/operateurs/publication/annexe-1-dispositif
[2] https://www.autoriteprotectiondonnees.be/publications/avis-n-108-2021.pdf
[3] https://academic.oup.com/cybersecurity/article/1/1/69/2367066

[4] https://www.globalencryption.org/2020/11/breaking-encryption-myths/

médecins, avocats, employés du secteur public, et contre les autres citoyens, ainsi que les entreprises et les institutions, y compris les gouvernements.

En plus d'introduire des portes dérobées dans des systèmes chiffrés de bout-en-bout existants, la Législation sur la conservation des données décourage les entreprises à offrir des nouveaux produits chiffrés de bout-en-bout. Comme nous l'avons observé dans d'autres pays qui ont introduit une législation similaire[5], la législation va voir un impact négatif sur la confiance dans les entreprises technologiques belges et va affecter leur compétitivité sur les marchés internationaux et européens. En outre, la législation pourrait engendrer un impact plus large sur le Marché Unique Numérique Européen, dans la mesure où les entreprises dans d'autres États Membres pourraient être contraintes de prendre en compte ces nouvelles exigences si elles veulent offrir leurs produits sur le marché belge.

Si le but recherché par la Législation sur la conservation des données est de renforcer la sécurité des belges, elle ne peut pas l'atteindre en ébranlant les fortes protections sur lesquelles nous nous reposons tous dans nos vies ; de sorte que le chiffrement de bout-en-bout ne devraient pas être menacé ou affaiblit par cette législation.

Signataires* :

Access Now
Adriaan Peeters
Africa Media and Information Technology Initiative (AfriMITI)
An Van Wesemael
AP2SI - Associação Portuguesa para a Promoção da Segurança da Informação
Bart Coppens, Professor, Ghent University
Bart Preneel, Prod. dr. ir., University of Leuven
Big Brother Watch
Blacknight Internet Solutions Ltd
Cédric Peeters, Vrije Universiteit Brussel (VUB)
Centre for Democracy and Technology
Citizen D/Državljan D
Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
ContactOffice
Cranium
Cybersecurity Advisors Network (CyAN)
Dieter Houthooft, IT Generators BV
Digital Infrastructure Association NL
Encryption Europe
European Digital Rights (EDRi)
Filip Lenaerts, CEO, Filip Lenaerts Corporation
Filip Schepers

[5] https://www.internetsociety.org/news/press-releases/2021/new-study-finds-australias-tola-law-poses-long-term-risks-to-australian-economy/

Geert Antheunis
Global Partners Digital
Global Voices
Guido De smet
Hannes De Bondt
Homo Digitalis
Immo Deprez
Instituto Beta: Internet & Democracia (Brasil)
Internet Freedom Foundation (IFF)
Internet Society
Internet Society Belgium Chapter
Internet Society Catalunya Chapter
Internet Society Democratic Republic of Congo Chapter
Internet Society Ghana Chapter
Internet Society Netherlands Chapter
Internet Society Portugal Chapter
ISOC India Delhi Chapter
Internet Society India Hyderabad Chapter
IP.rec - Law and Technology Research Institute of Recife
IT-Pol Denmark
JCA-NET
Jenne Tondeleir
Jens Finkhäuser, Interpeer Project
Jeroen Lambrichts, University of Hasselt
Jochen Timmerman
Joran Leenders
José Legatheaux Martins, Professor, Faculty of Sciences of NOVA University of Lisbon
Kijiji Yeetu
Kristof Dujardin
Kristof Provost, FreeBSD
Liga voor Mensenrechten
Mailfence
Mário Gaspar da Silva, Professor, Instituto Superior Técnico, Universidade de Lisboa, Portugal
Maarten De Bal
Mathias Bynens
Mega Limited
Merijn De Mil
Milton Mueller, Professor, Internet Governance Project, Georgia Institute of Technology
Netwerk Democratie
Onckelinx & Onckelinx BV
Open Governance Network for Europe

OpenMedia
OSCC BV Organization
Peter Vanderborght
Philippe Dreesen, Vrije Universiteit Brussel (VUB)
Privacy & Access Council of Canada
Quantum Leap Development
Ranking Digital Rights
RESPONSUM
Riana Pfefferkorn, Research Scholar, Stanford Internet Observatory
Sammi Fux
SFLC.in
Statewatch
Stijn Volckaert, Professor of Computer Science, KU Leuven
Suomen Internet-yhdistys - Internet Society Finland Chapter
The Electronic Privacy Information Center (EPIC)
Tresorit
Tutanota
Youth Forum for Social Justice

*Les affiliations sont reprises aux seules fins d'identification.