Sécurité des produits et protection des données : les assurer et les associer, ça coule de source

Pauline Meyer, le 15 décembre 2022

Le Contrôleur européen de la protection des données salue la proposition de loi sur la cyber-résilience. Il estime cependant que la protection des données personnelles devrait être mieux intégrée.

Opinion 23/2022 on the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

L'opinion du Contrôleur européen de la protection des données

Le 9 novembre 2022, le Contrôleur européen de la protection des données (*European Data Protection Supervisor, EDPS*) émet une opinion sur la proposition de loi sur la cyber-résilience. La proposition de loi vise à poser des exigences minimales de cybersécurité applicables aux produits comportant des éléments numériques.

La proposition de la Commission européenne relative à une nouvelle loi sur la cyber-résilience (*Proposal for a Cyber Resilience Act*, P-CRA) fait suite au constat selon lequel le niveau global de cybersécurité n'est pas suffisamment élevé, de même que le niveau de compréhension par les utilisateurs des produits comportant des éléments numériques (« *products with digital elements* »).

La P-CRA cherche à poser les conditions horizontales minimales pour que des produits comportant des éléments numériques moins vulnérables soient mis sur le marché et pour que les utilisateurs puissent prendre la cybersécurité en compte pour orienter leur choix et leur utilisation de tels produits. Ces produits vont des logiciels ou systèmes d'exploitation aux téléphones portables et ordinateurs.

Pour ce faire, la P-CRA introduit des exigences essentielles pour la conception, le développement et la production de tels produits. Elle pose aussi des exigences pour les processus de gestion de vulnérabilités durant tout leur cycle de vie et des obligations pour les acteurs économiques en relation avec ces dernières. Finalement, la P-CRA prévoit des règles pour

surveiller le marché et la conformité aux obligations susmentionnées.

La proposition de loi prend en compte la protection des données, notamment en imposant la prise en considération, pour déterminer le niveau de risque de cybersécurité d'un produit, des fonctions critiques ou sensibles comme le traitement de données (art. 6 let. c P-CRA). Les exigences de sécurité comprennent la protection de la confidentialité et de l'intégrité des données, notamment personnelles, ainsi que le principe de minimisation des données (Annexe I ch. 3 let. c, d et e en lien avec l'art. 5 par. 1 let. c RGPD).

L'EDPS salue la proposition et soutient son objectif général d'améliorer le fonctionnement du marché interne en posant un cadre légal uniforme en termes d'exigences minimales de cybersécurité pour les produits comportant des éléments numériques. La sécurité des données, figurant aux art. 5 par. 1 let. f RGPD et 32 RGPD, constitue l'un des principes cardinaux en protection des données. L'EDPS est donc satisfait des considérations de protection des données dans la proposition et estime que la cybersécurité contribue à la protection de la sphère privée.

En revanche, l'EDPS recommande que les exigences comprennent également la protection des données dès la conception et par défaut. Cette recommandation vaut principalement pour les fabricants de produits qui ne traitent pas eux-mêmes ensuite des données. Les fabricants se limitent en effet souvent à fournir un produit à des particuliers.

Le consid. 78 RGPD incite les fabricants à prendre en considération la protection des données lors de la conception de produits pour permettre aux responsables du traitement et aux sous-traitants d'assumer leurs obligations subséquentes. Il ne s'agit que d'une incitation pour les fabricants qui ne traitent pas de données personnelles. Selon l'EDPS, il est nécessaire que la protection des données par défaut et dès la conception soit exigée dans la P-CRA dès le début du cycle de vie d'un produit.

L'EDPS formule deux commentaires spécifiques au sujet du champ d'application de la P-CRA. D'une part, il lui semblerait judicieux d'expliquer dans le préambule de la P-CRA l'importance, en cybersécurité et en protection des données, des produits numériques servant à des opérations cryptographiques (comme le chiffrement, en transit ou au repos, ou la pseudonymisation). L'EDPS souhaite par ailleurs que le matériel de cryptographie soit considéré comme critique (par son ajout à la classe II de l'annexe III) et qu'il soit par conséquent sujet à des procédures d'analyse de risque plus strictes.

D'autre part, l'EDPS recommande que la P-CRA clarifie sa relation avec d'autres législations.

Par exemple, les dispositifs médicaux sont exclus de la proposition car soumis à une réglementation spécifique (cf. Règlement (UE) 2017/745). Néanmoins, celle-ci ne prévoit pour l'EDPS pas d'exigences suffisantes en termes de cybersécurité et de protection des données, raison pour laquelle son application ne devrait pas être exclue de l'application de la P-CRA.

Pour l'EDPS, les synergies entre la P-CRA et le RGPD conformément au consid. 17 doivent se répercuter dans la loi. Concrètement, la P-CRA doit prévoir les aspects relatifs à la création de synergies en termes de standardisation et certification, par exemple lorsqu'il en va de l'échange d'information. En outre, la proposition doit clarifier qu'elle n'affecte ni les réglementations préexistantes de protection de données ni les pouvoirs des autorités de surveillance en vertu de celles-ci.

L'EDPS soutient la reconnaissance par la P-CRA du traitement de données comme une fonction critique et sensible susceptible de justifier une certification de cybersécurité. Il lui importe toutefois de clarifier qu'une telle certification n'équivaut pas en soi à une conformité au RGPD.

L'EDPS salue finalement les sanctions proposées à l'art. 53 P-CRA, similaires à celles prévues par le RGPD. Pour non-conformité aux exigences essentielles de l'Annexe I ou aux obligations de fabricants, la P-CRA habilite les autorités de surveillance du marché désignées par les États membres à infliger des amendes administratives allant jusqu'à 15 millions d'euros ou jusqu'à 2.5% du revenu global. En cas de non-conformité à d'autres obligations de la P-CRA, l'amende peut se monter à 10 millions d'euros ou 2% du revenu global. L'amende peut atteindre 5 millions d'euros ou 1% du revenu global pour l'information incorrecte ou incomplète faisant suite à la requête d'une autorité d'application de la loi.

La situation en Suisse

Le droit suisse ne prévoit actuellement pas de réglementation spécifique de cybersécurité pour les produits à composantes numériques ou pour les fabricants de tels produits. Il n'existe en effet à notre connaissance aucun instrument légal imposant des exigences minimales en termes de cybersécurité aux fabricants et autres intervenants dans le cycle de vie de tels produits, sous réserve des considérations de la Loi sur la sécurité des produits (LSPro). Elles se limitent à assurer la sécurité physique et la santé des utilisateurs.

D'autres réglementations s'appliquant à un cercle spécifique de produits se limitent au renvoi ponctuel à des considérations très générales de cybersécurité, comme l'art. 4 de l'Ordonnance sur les dispositifs médicaux (ODim) qui renvoie au Règlement (UE) 2017/745

susmentionné.

Par ailleurs, la LPD, comme le RGPD, se limite à imposer des obligations de protection des données uniquement aux personnes traitant de telles données. Partant, le fabricant qui se limite à la mise sur le marché de produits utilisés ensuite par d'autres personnes n'est pas soumis en tant que tel à des obligations de protection des données.

L'art. 7 nLPD imposant au responsable du traitement de garantir la protection des données dès la conception et par défaut, il serait judicieux de prévoir en droit suisse des obligations applicables également aux fabricants, afin d'une part de ne pas surcharger les responsables du traitement qui traitent des données par le biais de produits fabriqués par des tiers et, d'autre part, de n'exclure aucune étape du cycle de vie d'un produit comportant des éléments numériques.

Proposition de citation : Pauline MEYER, Sécurité des produits et protection des données : les assurer et les associer, ça coule de source, 15 décembre 2022 *in* www.swissprivacy.law/190