Interpellation Jean-Christophe

Vol et perte de données de clients ou de collaborateurs, notamment de numéros AVS : La loi suisse est-elle suffisante?

- Les entreprises et collectivités publiques ou parapubliques qui traitent des données personnelles ont-elles l'obligation d'informer les personnes dont elles traitent les données en cas de vol ou de perte de données, notamment sensibles ? Si non, le Conseil fédéral envisage-t-il d'inscrire une telle obligation dans la LPD ou toute autre législation idoine?
- Quelles obligations ces entreprises et collectivités ont-elles envers les personnes dont les données ont été volées ou perdues? Doivent-elles notamment tout mettre en œuvre pour éviter l'usurpation d'identité? Doivent-elles prendre en charge tous les frais qui découlent du vol ou de la perte des données (notamment les démarches administratives pour obtenir de nouvelles données)?
- Le droit du travail (privé et public) est-il en particulier suffisant pour protéger les travailleurs dont l'employeur se fait voler ou perd les données que la loi l'autoriser à traiter?
- Quelles mesures existe-t-il en cas de vols de numéro AVS, notamment en vue de prévenir l'usurpation d'identité ou l'abus de prestations?
- L'AVS a-t-elle notamment l'obligation de fournir un nouveau numéro AVS en cas de vol de données (en particulier en cas de risque d'usurpation d'identité)? Si non, pourquoi? Le Conseil fédéral compte-t-il combler cette lacune?
- La législation en vigueur est-elle suffisante en cas de vol ou de perte de données bancaires, notamment en vue de prévenir l'usurpation d'identité?
- La sécurité des systèmes informatiques des banques, que cela soit au niveau des sites internet, des sites de e-banking ou du systèmes cœur, est-elle assurée ? Par qui sont-ils vérifiés et contrôlés? Peut-il y avoir une sanction en cas de défaut de sécurité informatique d'une banque?
- Le Conseil fédéral est-il prêt à étudier ces problèmes en détails dans le cadre de sa réponse à la motion 14.3288?

Développement

Les récentes attaques informatiques contre la BCGE, Sony, JPMorganChase ou Home Depot ont montré que des pirates pouvaient dérober des milliers, voire des millions de données de clients ou de collaborateurs, parmi lesquelles des données éminemment sensibles comme des numéros de sécurité sociale ou de compte bancaire. Il est malheureusement à craindre que ces attaques se multiplient et que leur ampleur s'aggrave. D'autres entreprises qui traitent des données sensibles de leurs clients ou collaborateurs les perdent. Parmi les désagréments que subissent les victimes, il y a notamment le risque accru d'usurpation d'identité. Certaines victimes doivent notamment faire appel à des sociétés spécialisées contre ce risque, sans que l'entreprise qui traitait leurs données et se les ai fait dérober ne prenne ces frais importants en charge.

22.2.2015