Recyclé en violation de sécurité

David Dias Matos, le 30 août 2023

L'autorité espagnole de protection des données estime que la Direction générale de la police commet une violation de la sécurité des données en recyclant des documents internes en blocs-notes accessibles au public.

Décision de l'autorité de protection des données d'Espagne du 21 février 2023 (PS-00480–2022)

Lors d'une visite dans un poste de police, un résident espagnol remarque des blocs-notes sur le guichet de la réception. Au verso des feuilles attachées ensemble se trouvent des données personnelles concernant à la fois les citoyens qui se sont rendus au poste de police et les fonctionnaires de police qui y travaillent.

À la suite de cette trouvaille, le résident alerte l'autorité espagnole de la protection des données (*Agencia Española de Protección de Datos*, « AEPD ») de la situation en déposant une plainte contre la Direction générale de la police. Il y joint plusieurs photographies montrant les versos où peuvent se lire noms, prénoms et numéros d'identification d'individus, certains comprenant le sceau du ministère de l'intérieur espagnol. L'enquête a démontré que ces blocs-notes étaient issus de papiers recyclés par le poste de police.

Dans sa décision, l'AEPD estime préalablement que c'est bien la Direction générale de la police espagnole (« DGP ») et non le poste de police en tant que tel qui détermine les finalités et les moyens. Partant, c'est elle la responsable du traitement de données personnelles.

Ensuite, l'AEPD rappelle la définition générale de la violation de données à caractère personnel ou « violation de sécurité ». L'art. 4 par. 12 RGPD la définit comme

> « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ».

En l'espèce, l'AEPD juge qu'une violation de la sécurité a bien eu lieu. Le fait que la plaignante ait eu accès à des blocs-notes contenant des données personnelles tant d'agents de police que de personnes qui se sont adressées à eux est constitutif d'une violation de sécurité par divulgation non autorisée.

L'AEPD rappelle ensuite que l'identification d'une violation de sécurité n'implique pas automatiquement l'imposition d'une sanction. Il est encore nécessaire d'analyser la diligence dont le responsable du traitement a fait preuve ainsi que les mesure de sécurité appliquées.

Pour ce faire, l'AEPD analyse successivement les art. 5 et 32 ss du RGPD. L'art. 5 let. f RGPD traite des sous-principes au principe de sécurité des données, à savoir l'intégrité et la confidentialité. Il prévoit que les données à caractère personnel sont

> « traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées ».

En l'espèce, l'AEPD estime que le principe de confidentialité a été violé. En effet, il est établi que les données personnelles des personnes concernées contenues dans la base de données de la DGP ont été indûment exposées à des tiers non autorisés.

Ensuite, l'AEPD se penche sur le principe de sécurité des données et plus particulièrement du traitement de l'art. 32 RGPD. Son par. 1 prévoit que

> « compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (…) ».

Après avoir été interrogée par l'AEPD sur les mesures mises en place pour garantir la sécurité, la DGP l'a informé que le commissariat disposait de quatre déchiqueteuses à papier, ainsi que de directives internes relatives à la destruction de documents de police. Elle ajoute

que la confidentialité et la destruction correcte des documents de police sont des « objectifs prioritaires pour la DGP ». Cet engagement se traduit par l'élaboration de règlements et leur diffusion, ainsi que la formation des agents et des procédures disciplinaires en cas de violation.

Cependant, l'AEPD a jugé ces mesures insuffisantes, étant donné que des documents contenant des informations personnelles n'ont pas été détruits mais recyclés en blocs-notes et rendus accessibles pour des tiers.

L'AEPD conclut donc à la violation tant des principes de l'art. 5 let. f RGPD que des obligations des art. 32 ss RGPD. Bien que ces violations aient été jugées graves par l'AEPD, le droit national espagnol ne permet pas à des organes publics d'être sanctionnés par des amendes administratives. L'AEPD s'est donc limitée à réprimander le responsable du traitement.

Cette décision *a priori* anecdotique illustre bien la rapidité et le caractère aléatoire de la survenance d'une violation de sécurité. Sans doute, la démarche de réutilisation de papier est partie d'une intention écologique (voire économe). Elle n'a toutefois pas été sans (graves) conséquences.

Le droit suisse prévoit également le principe de sécurité des données à l'art. 8 LPD (anciennement art. 7 aLPD) pour le responsable du traitement et les sous-traitants. Des mesures techniques et organisationnelles seront à mettre en place pour assurer une sécurité adéquate des données personnelles par rapport au risque encouru.

Conformément au mandat donné au Conseil fédéral à l'art. 8 al. 3 LPD, les art. 1 à 6 OPDo ont été adoptés. Ils exposent d'abord les principes (art. 1 OPDo) et les objectifs de la sécurité des données (art. 2 OPDo). L'art. 3 OPDo liste ensuite les mesures à mettre en place selon les objectifs de protection, comme le contrôle de l'accès aux données (art. 3 al. 1 let. a OPDo).

Cette décision met en exergue le fait que la simple mise en place de mesures techniques et organisationnelles ne suffit pas toujours. D'une part, la LPD ne prévoit pas d'exigence de sécurité absolue, car le risque zéro n'existe pas. D'autre part, il est possible de prévoir et de mettre en place un grand nombre de mesures, ici des déchiqueteuses et des formations, encore faut-il qu'elles soient mises en œuvre. La sécurité des données est par conséquent un processus dynamique. Les mesures doivent régulièrement être réexaminées et, le cas échéant, adaptées pour maintenir un niveau de sécurité adéquat.

_swissprivacy.law

Proposition de citation : David Dias Matos, Recyclé en violation de sécurité, 30 août 2023 *in* www.swissprivacy.law/247

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.