ISABELLE DUBOIS

Avocate de formation et ancienne juge cantonale, Isabelle Dubois a été la première préposée à la protection des données et à la transparence du canton de Genève. Elle met depuis janvier 2014 son expertise en la matière à disposition des organisations comme indépendante à l'enseigne d'Isabelle Dubois, AD HOC RESOLUTION, et délivre expertises et accompagnements en la matière. Elle exerce la fonction de DPO externe et enseigne la protection des données dans le cadre de formations dispensées par l'Université de Genève et par les HES-SO de Lausanne et Sierre.

www.adhocresolution.ch

AD HOC RESOLUTION

LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES DE L'UNION EUROPÉENNE ET LA DIRECTIVE « POLICE-JUSTICE »

Présentation sous forme d'entretien avec Isabelle Dubois, AD HOC RESOLUTION, expert en protection des données et ancienne préposée cantonale

Vous aviez présenté le RGPD à Pixel juste avant son entrée en vigueur. Ce règlement est complété par une directive dite « Police-Justice ». De quoi s'agit-il ?

La Directive 95/46 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel, à l'instar du Règlement (RGPD) qui l'a remplacée dès 2016, ne s'applique pas au traitement de données à caractère personnel mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que les activités dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière. C'est pourquoi une directive règle spécifiquement le traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales. Elle a pour but, comme indiqué dans les motifs, de « contribuer à la réalisation d'un espace de liberté, de sécurité et de justice ». L'enjeu est majeur car les nouvelles technologies permettent de multiplier les modes de traitement des données et de collecter et transmettre une quantité quasi illimitée de données en un temps record. Il faut donc à la fois faciliter le flux de données entre les autorités compétentes des Etats membres et assurer un niveau élevé et homogène de protection des données à caractère personnel.

Est-ce que cette Directive s'applique uniquement aux autorités de police ?

Non, son champ d'application est plus large que cela : les autorités compétentes en question comprennent non seulement les autorités publiques telles que les autorités judiciaires, la police ou d'autres autorités répressives mais aussi tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique aux fins de la présente directive. Lorsqu'un tel organisme traite des données à caractère personnel à des fins autres que celles prévues dans la présente directive, c'est le RGPD qui s'applique.

RGPD et Directive Police-Justice peuvent donc s'appliquer tous deux à un même organisme, mais à des traitements différents. Par exemple, les établissements financiers conservent, à des fins de détection ou de poursuites d'infractions pénales ou d'enquêtes en la matière, certaines données qu'ils ne transmettent aux autorités nationales compétentes que dans des cas spécifiques. Un organisme qui traite ces données pour le compte de ces autorités est lié par la présente directive (voir les dispositions applicables aux sous-traitants) et par le RGPD pour les autres traitements de données à caractère personnel.

A noter que la présente directive reprend les mêmes définitions, notions, et principes applicables que le RGPD, de même que la plupart des obligations pour le responsable de traitement, mais leur champ d'application est différent et complémentaire. De plus, alors que le RGPD s'applique de plein droit aux Etats membres, la présente directive donne instruction aux Etats membres de légiférer dans le sens indiqué. Elle a été transposée en France au sein du Titre III (chapitre 1 à 4, art. 87 à 114) de la loi Informatique et Libertés.

Y a-t-il des obligations pour le Responsable de traitement qui sont spécifiques à cette directive ?

Oui, il s'agit des obligations suivantes :

- Etablir une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées : les personnes suspectées d'infraction pénale, les personnes reconnues coupables d'une infraction pénale, les personnes victimes d'une infraction pénale, et les tiers à une infraction pénale (contacts, témoins, etc.)
- Distinguer les données à caractère personnel fondées sur des faits des données fondées sur des appréciations personnelles
- Vérifier la qualité des données avant toute communication et mise à disposition
- Le traitement doit être licite et donc être nécessaire pour remplir une mission effectuée par une autorité compétente, pour les finalités prévues par la présente directive
- Le traitement portant sur des données à caractère particulier (dites aussi sensibles : qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle) n'est autorisé qu'en cas de nécessité absolue et s'il est autorisé par le droit de l'Union ou le droit d'un État membre, qu'il s'agit de protéger les intérêts vitaux ou que les données ont manifestement été rendues publiques par la personne concernée.

Est-ce que le droit d'accès pour les personnes concernées est identique à celui prévu par le RGPD ?

Non, il connaît certaines limitations dues aux finalités spécifiques du traitement prévu par la Directive et mentionnées par elle, pour éviter par exemple de gêner des enquêtes, des recherches ou des procédures judiciaires, ou éviter de nuire à la prévention ou à la détection d'infractions pé-

nales. Par ailleurs, la portabilité n'est pas prévue. Vos lecteurs trouveront ici le lien sur la Directive, ainsi que les explications résumées de la CNIL :
https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016L0680&from=FR
https://www.cnil.fr/fr/directive-police-justice-de-quoi-parle-t

Et s'agissant du code de sécurité intérieure, quel est l'impact des nouvelles normes européennes pour les systèmes installés sur la voie publique et dans les lieux ouverts au public ?

Pour répondre à cette question il faut rappeler que le RGPD vise un traitement des données personnelles conforme et unifié, et de ce fait, une libre circulation des données personnelles au sein de l'Union, et s'applique à tout traitement de données personnelles, sauf dans les domaines qui ne sont pas du droit de l'Union. La sécurité fait l'objet d'un programme européen, qui prévoit 3 priorités et 5 principes : Le respect absolu des droits fondamentaux, la formulation transparente et responsable des politiques de sécurité, une recherche de l'efficience par plus de collaboration opérationnelle et de nouveaux financements et formations, une meilleure coordination des agences de l'UE, et des actions de sécurité interne et externe conjointes. Les priorités sont le terrorisme et la radicalisation, la criminalité organisée internationale et la cybersécurité.

Certes le RGPD ne va dire aux pays de l'Union comment mettre en œuvre ce programme, mais il leur impose, ce faisant, de traiter les données personnelles d'une manière conforme. La France a adopté la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, qui liste toutes les modifications générales ou spécifiques des lois nécessitées par le RGPD, essentiellement la loi informatique et libertés qui a été mise à jour.

Par conséquent, les concepts et obligations prévues par le RGPD pour le responsable de traitement s'appliquent à tout nouveau traitement de données personnelles par une municipalité. C'est ainsi, comme le rappelle la CNIL[1], qu'une analyse d'impact devra être effectuée car un dispositif de vidéoprotection conduit à « la surveillance systématique à grande échelle d'une zone accessible au public », type de traitement expressément mentionné à l'article 35.1 du RGPD comme susceptible de présenter un risque élevé. De même, tout système doit être conçu selon le principe de la protection des données dès la conception et par défaut, pour permettre au responsable de traitement de respecter ses obligations en protection des données ; enfin, et les informations prévues par l'art. 13 RGPD et 104 de la loi informatique et libertés devront être fournies à la personne concernée.

Propos reccueillis par Rémi Fargette, AN2V

1. https://www.cnil.fr/fr/la-videosurveillance-videoprotection-sur-la-voie-publique