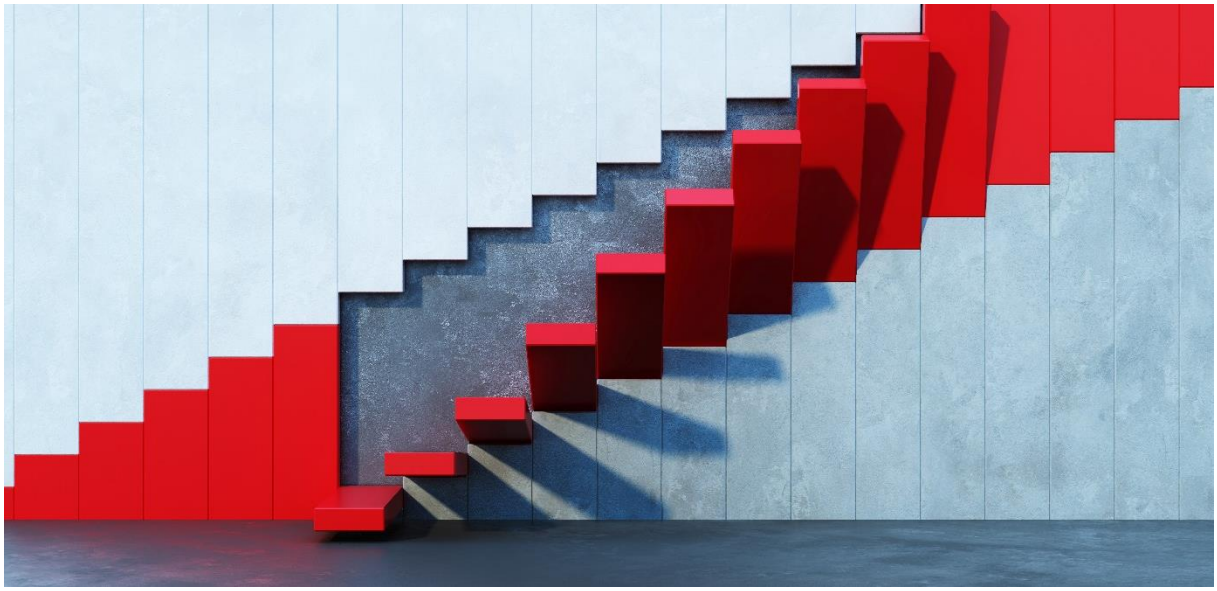
racine AVOCATS

Flash Info

07 novembre 2018



Publication par la Cnil d'une liste de 14 traitements soumis à analyse d'impact

Contexte

Parmi les innovations du RGPD figure en bonne place « l'analyse d'impact », autrement appelée PIA ou par la Cnil elle-même AIDP.

Lorsqu'un type de traitement, en particulier par le recours à des nouvelles technologies et compte tenu de la nature, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable de traitement effectue, avant le traitement, une analyse d'impact des opérations de traitement envisagées.

Cette analyse d'impact contient au moins une description systématique des opérations de traitement, une évaluation de la nécessité et de la proportionnalité des opérations au regard des finalités ainsi qu'une évaluation des risques et les mesures envisagées pour faire face à ces risques.

L'analyse d'impact peut s'accompagner d'une consultation préalable de la Cnil.

Le RGPD prévoit 3 cas dans lesquels l'analyse d'impact est impérative :

- Cas 1 – l'évaluation systématique et approfondie d'aspects personnels, y compris, dit le texte, « le profilage »

- Cas 2 – le traitement à grande échelle de données sensibles au sens de l'article 9 (origine raciale, ethnique, opinion politique, religieuse, philosophique, appartenance syndicale, génétique biométrique, …)
- Cas 3 – la surveillance à grande échelle d'une zone accessible au public (essentiellement la vidéo protection).

Liste CNIL

Mais l'article 35 du RGPD prévoyait aussi que l'autorité nationale de contrôle (chez nous la Cnil) puisse établir et publier une liste type d'opérations de traitement pour lesquels une analyse relative à la protection des données est requise. En l'occurrence, cette liste a été publiée le 6 novembre 2018 par la Cnil.

On peut distinguer dans cette liste les traitements que l'on peut qualifier de « sectoriels » c'est-à-dire qui s'appliquent surtout à des secteurs d'activité en particulier, et les traitements « génériques » qui eux s'appliquent à toutes les entreprises.

Pour les traitements sectoriels, on notera surtout les établissements de santé, les traitements relatifs à la génétique, les entreprises de transport pour l'usage de chronotachygraphes, les banques et sociétés de crédit pour le scoring, ou les moyens de lutte contre la fraude aux moyens de paiements, les sociétés d'assurance sur les vérification d'antécédents, établissements du logement social pour les traitements relatifs à l'instruction des demandes de logements, etc.

Le monde du web n'est pas épargné par cette liste. On retiendra que sont notamment concernés les réseaux sociaux pour les traitements reposant sur une analyse comportementale visant à détecter des comportements « interdits » ainsi que les courtiers en données (data brockers) et les professionnels de la publicité personnalisée en ligne s'agissant de l'ensemble de leurs traitements.

Mais toutes les entreprises peuvent être visées par les traitements génériques soumis à un PIA, et notamment :

- Ressource humaines :
    - Traitement spécifiques aux « hauts potentiels »
    - Recrutement via un algorithme
    - Plan de formation via algorithme
    - Outils de détention et de prévention des « départ de salariés »

- Sécurité de l'entreprise :
    - Outils de cyber surveillance – la Cnil donne en exemple « l'analyse de mails sortant pour identifier les fuites d'information » (data lost prevention)
    - Vidéosurveillance d'employés manipulant de l'argent
    - Vidéosurveillance d'un entrepôt stockant des biens de valeur

- Prévention :
    - Dispositifs de recueil d'alertes professionnelles
    - Dispositifs de recueil de signalements concernant des faits de trafic d'influence ou de corruption ;
    - Dispositif d'alerte mis en œuvre dans le cadre du droit de vigilance

Impact sur votre entreprise

Les entreprises visées par les traitements dits « sectoriels » n'ont d'autre choix que de procéder à des PIA, sans délai pour les nouveaux traitements et dans un délai maximum de 3 ans (délai accordé par la Cnil) pour les traitements existants avant le 25 mai 2018.

Pour les traitements génériques, il appartient à chaque entreprise ou acteur public de contrôler qu'il ne met pas en œuvre un tel traitement et, le cas échéant, de mettre en œuvre ces PIA dans les mêmes délais.

Point d'attention 1 – Le fait que cette liste soit publiée n'exonère pas l'entreprise de faire une analyse plus globale et de voir si d'autres traitements ne sont pas éligibles à un PIA. La liste est donc une liste minimum ;

Point d'attention 2 - L'analyse d'impact n'est pas une analyse de risque technique… L'analyse d'impact est avant tout une étude juridique.

Il s'agit de contrôler si pour un traitement X l'ensemble du RGPD est bien respecté notamment les principes généraux : légalité, licéité, proportionnalité, durée,… les principes tels que la minimisation ou la mise en œuvre d'un process de privacy by design, les conditions et modalités d'exercice du droit des personnes, etc.

Les consultants en sécurité sont les bienvenus dans le monde des analyses d'impact mais ils ne peuvent à eux seuls répondre aux exigences du RGPD qui va bien au-delà de l'analyse de risque ou de vulnérabilité.

Point d'attention 3 - Cas particulier des groupes internationaux. La liste publiée par la Cnil vise les entreprises soumises à la règlementation française. Mais ce qui est vrai pour la Cnil est vrai pour les autres autorités de contrôle. Il revient à chacune d'elle de dresser sa propre liste. De fait les groupes internationaux seront vraisemblablement soumis à des listes différentes selon leur lieu d'implantation. Il leur reviendra donc de faire une analyse cumulée des listes des 29 autorités de contrôle, nonobstant le choix d'une autorité chef de file.

AUTEURS

Eric Barbry

Avocat Associé

ebarbry@racine.eu

Léa Paravano

Avocat

lparavano@racine.eu