Privacy Shield : l'UE et les États-Unis ne sont pas encore sur la même ligne

Le choix d'un processus d'autocertification est susceptible de responsabiliser les entreprises, mais il implique de fournir des informations claires, notamment sur les possibilités, pour un individu, de s'opposer au traitement de ses données.

Le groupe de travail Article 29, qui réunit la CNIL et ses homologues des États membres de l'Union européenne, établit ce constat dans un rapport consécutif à l'examen, les 18 et 19 septembre derniers à Washington, du **Privacy Shield**.

Huit de ses représentants ont pris part, aux côtés du gouvernement américain et de la Commission européenne, à la première évaluation annuelle de ce dispositif destiné à encadrer les flux transatlantiques de données personnelles.

Adopté par Bruxelles le 12 juillet 2016 et entré en vigueur le 1er août de la même année, le texte succède au Safe Harbor, que la Cour de justice de l'Union européenne avait invalidé le 6 octobre 2015 dans le cadre d'une procédure intentée contre Facebook par un résident autrichien.

Il constitue une « décision d'adéquation » par laquelle les 28 États membres de l'UE – auxquels s'ajoutent la Norvège, le Liechtenstein et l'Islande, sous l'égide du groupe « Article 31 » – reconnaissent que les États-Unis apportent un niveau suffisant de protection des données personnelles.

En conséquence, sous réserve de répondre aux exigences inscrites dans le texte, une entreprise peut transférer, sans restrictions, des données de citoyens européens vers l'autre côté de l'Atlantique.

Données RH : des interprétations divergentes

Article 29 reconnaît que des structures et des procédures ont été mises en place pour assurer un bon fonctionnement du Privacy Shield, mais déplore de nombreux aspects à améliorer.

La nécessité pour les autorités U.S. de fournir des « informations claires » est d'autant plus prégnante que 83 % des quelque 2 500 organisations ayant adhéré au dispositif l'ont fait sur la base d'un examen conduit intégralement en interne.

Article 29 demande par là même à Washington de renforcer ses mécanismes de contrôle de conformité, dans une logique anticipatrice plutôt que correctrice.

L'administration américaine est également interpellée sur sa perception des relations entre les responsables du traitement de données basés dans l'UE et leurs sous-traitants établis aux États-Unis ; plus particulièrement sur un volet : les « données RH ».

Sur place, le département du Commerce (DoC) a repris l'approche du Safe Harbor en considérant que le traitement, aux États-Unis, de données relatives aux employés d'une société établie dans

l'UE, est de nature commerciale. Si bien que les CNIL européennes ne sont pas compétentes en cas de litige.

Collectes massives : les craintes des CNIL

Sur l'accès aux données par les autorités, Article 29 salue des « efforts de transparence » marqués entre autres par la déclassification de certaines décisions prises au nom du FISA (Foreign Intelligence Surveillance Act).

Le Congrès débat actuellement d'une réforme de ce texte sur lequel le renseignement U.S. s'appuie pour obtenir un droit de regard sur les données de citoyens européens transférées vers les États-Unis sous le couvert du Privacy Shield.

La section 702, dont dépendent les programmes de surveillance PRISM et UPSTREAM, doit faire l'objet d'une revalidation pour le 1er janvier 2018.

Notant que dans le cadre de ces programmes, les activités de surveillance sont dites « ciblées dans la mesure du possible », mais que le gouvernement américain n'en a pas, lors de la réunion à Washington, apporté de preuve formelle, Article 29 l'enjoint à s'engager légalement, non sans profiter de la réforme du FISA pour introduire de garde-fous tels qu'un « motif raisonnable de suspicion ».