# ARTICLE

## SANCTIONS DES ORGANISMES EN CAS DE VIOLATIONS CONSTATÉES, QUELLE EST LA MARGE D'APPRÉCIATION DONT DISPOSENT LES AUTORITÉS DE PROTECTION DES DONNÉES ?

IT et données personnelles Droit de la propriété intellectuelle, média et art | 10/01/25 | Florence Chafiol
Alexandra Antalis

Dans un arrêt en date du 26 septembre 2024[1], la Cour de justice de l'Union européenne (« **CJUE** ») a indiqué que l'autorité de protection des données qui constate une violation avérée des dispositions relatives à la protection des données à caractère personnel, n'est pas tenue d'adopter dans tous les cas une mesure correctrice au titre de l'article 58, paragraphe 2, du Règlement général sur la protection des données (« **RGPD** »)[2] en particulier une amende administrative.

*Résumé des faits*

Le 15 novembre 2019, un organisme notifie une violation de données à caractère personnel à l'autorité de protection des données compétente (Commissaire à la protection des données et à la liberté de l'information pour le Land de Hesse, Allemagne) car une employée avait consulté à plusieurs reprises des données à caractère personnel d'un client de l'organisme.

L'organisme décide de ne pas communiquer la violation à la personne concernée.

La personne concernée prend incidemment connaissance du fait que ses données à caractère personnel ont été indûment consultées. Elle introduit une réclamation auprès de l'autorité de protection des données compétente notamment pour (i) manquement à l'obligation de communiquer la violation de données à caractère personnel[3] et (ii) manquement à l'obligation d'assurer la sécurité des données[4], en reprochant à l'organisme la durée de conservation des journaux (trois mois en l'espèce[5]) et la gestion des habilitations.

A la suite de la réclamation, l'autorité de protection des données compétente entend l'organisme qui a indiqué ne pas avoir procédé à une communication de la violation de données à caractère personnel car son délégué à la protection des données avait estimé qu'il n'y avait pas de risque élevé pour les droits et les libertés de la personne concernée. En effet, (i) des mesures disciplinaires avaient été prises contre l'employée, (ii) l'employée avait confirmé par écrit qu'elle n'avait ni copié ni conservé les données à caractère personnel, qu'elle ne les avait pas transmises à des tiers et qu'elle ne le ferait pas à l'avenir.

Par une décision du 3 septembre 2020, l'autorité de protection des données compétente considère que l'organisme n'a pas enfreint l'article 34 du RGPD puisque même si les données avaient été consultées par l'employée, rien n'indiquait que celle-ci les avait transmises à des tiers ou les avait utilisées au détriment de la personne concernée. Elle précise également qu'un contrôle de principe de chaque accès aux documents n'est pas nécessaire puisque des droits d'accès étendus peuvent, en principe, être accordés à des salariés à condition qu'ils soient informés des conditions dans lesquelles ils peuvent accéder aux documents.

La personne concernée introduit un recours contre la décision prise par l'autorité de protection des données compétente devant le tribunal administratif compétent (Tribunal administratif de Wiesbaden, Allemagne). Elle considère qu'elle aurait dû infliger une amende administrative à l'organisme.

Le tribunal administratif allemand décide de poser la question préjudicielle suivante à la CJUE : « *Les dispositions combinées de l'article 57, paragraphe 1, sous a) et f), de l'article 58, paragraphe 2, sous a) à j), et de l'article 77, paragraphe 1, du [RGPD] doivent-elles être interprétées en ce sens que l'autorité de contrôle est toujours tenue d'intervenir au titre de l'article 58, paragraphe 2, [de ce règlement] lorsqu'elle constate un traitement de données qui empiète sur les droits de la personne concernée ?* ».

Autrement dit, le tribunal s'interroge sur le point de savoir si en cas de violation avérée de dispositions relatives à la protection de données à caractère personnel, le RGPD doit être interprété en ce sens que l'autorité de protection des données est tenue d'adopter des mesures correctrices telle une amende administrative, ou bien en ce sens que cette autorité dispose d'un pouvoir d'appréciation qui l'autorise, selon les circonstances, à s'abstenir de prendre de telles mesures.

*Appréciation de la CJUE*

La CJUE indique que le RGPD laisse à l'autorité de protection des données une marge d'appréciation quant à la manière dont elle doit remédier à l'insuffisance constatée et garantir le plein respect du RGPD.

En effet, l'article 58, paragraphe 2 du RGPD confère à l'autorité le pouvoir d'adopter diverses mesures correctrices. A cet égard, la Cour rappelle l'arrêt du 16 juillet 2020 (Facebook Ireland et Schrems, C-311/18, point 112) dans lequel elle a considéré que le choix du moyen approprié et nécessaire relève de l'autorité de protection des données, qui doit opérer ce choix en prenant en considération toutes les circonstances du cas concret et en s'acquittant avec toute la diligence requise de sa mission consistant à veiller au plein respect du RGPD.

La marge d'appréciation laissée à l'autorité est cependant limitée par la nécessité de garantir un niveau cohérent et élevé de protection des données à caractère personnel par une application rigoureuse des règles.

S'agissant, plus particulièrement, des amendes administratives, la Cour précise qu'elles sont imposées, selon les caractéristiques propres à chaque cas d'espèce, en complément ou à la place d'autres mesures correctrices. En outre, pour décider s'il y a lieu d'imposer une amende administrative et pour décider de son montant, l'autorité de protection des données doit dûment tenir compte de différents éléments, tels que la nature, la gravité et la durée de la violation.

> Par conséquent, il ne saurait être déduit ni de l'article 58, paragraphe 2, du RGPD ni de l'article 83 du RGPD l'existence d'une obligation à la charge de l'autorité de protection des données d'adopter, dans tous les cas, lorsqu'elle constate une violation de données à caractère personnel, une mesure correctrice, en particulier une amende administrative.

La personne concernée ne dispose pas d'un droit subjectif à voir l'autorité de protection des données imposer une amende administrative au responsable du traitement.

La Cour précise toutefois que l'autorité de protection des données est tenue d'intervenir lorsque l'adoption de l'une ou plusieurs des mesures correctrices est, compte tenu de toutes les circonstances du cas d'espèce, appropriée, nécessaire et proportionnée pour remédier à l'insuffisance constatée et garantir le plein respect du RGPD. Cependant, l'adoption d'une mesure correctrice peut, à titre exceptionnel et compte tenu des circonstances particulières du cas d'espèce, ne pas s'imposer lorsque trois conditions cumulatives suivantes sont réunies :

- La situation de violation du RGPD a déjà été rétablie,
- La conformité des traitements de données à caractère personnel au RGPD est assurée, et
- L'abstention de prononcer une mesure correctrice n'est pas de nature à porter atteinte à l'exigence d'une application rigoureuse des règles prévues par le RGPD.

Tel pourrait être le cas, notamment, lorsque le responsable du traitement, qui avait, en principe, mis en œuvre des mesures techniques et organisationnelles appropriées, a, dès qu'il a eu connaissance de cette violation, pris les mesures appropriées et nécessaires pour remédier à la violation conformément aux obligations qui lui incombent en vertu du RGPD.

Le tribunal administratif allemand devra maintenant vérifier que l'autorité de protection des données a procédé au traitement de la réclamation concernée avec toute la diligence requise et si, en adoptant la décision en cause au principal, elle a respecté les limites de la marge d'appréciation que lui confère l'article 58, paragraphe 2, du RGPD.

---

[1] Arrêt de la CJUE (TR et Land Hessen, C-768/20).

[2] Article relatif aux pouvoirs dont disposent les autorités de protection des données et notamment des pouvoirs d'enquêter et d'adopter des mesures correctives.

[3] Article 34 du RGPD.

[4] Article 32 du RGPD.

[5] La CNIL préconise dans son guide sur la sécurité des données personnelles de conserver les journaux sur une période glissante comprise entre six mois et un an (sauf, par exemple, en cas d'obligation légale portant sur cette durée de conservation, de besoin de gestion des contentieux, de contrôle interne ou encore d'un besoin identifié d'analyse post-incident).