_swissprivacy.law

Faute présumée du responsable de traitement en cas de cyberattaque

Charlotte Beck, le 31 mai 2023

Les questions préjudicielles posées par la Cour suprême administrative bulgare à la CJUE visent à déterminer les conditions dans lesquelles une réparation du préjudice moral peut être obtenue par la personne concernée dont les données ont été publiées sur Internet suite à une cyberattaque.

Conclusions de l'avocat général M. Giovanni Pitruzzella du 27 avril 2023, Affaire de la Cour de justice de l'Union européenne (CJUE) C-340/21, VB c. Natsionalna agentsia za prihodite

Le 27 avril 2023, l'avocat général Pitruzzella rend ses conclusions dans l'affaire C-340/21. Les faits concernent l'agence nationale des recettes publiques bulgare (*Natsionalna agentsia za prihodite,* NAP), qui subit une cyberattaque à la suite de laquelle des données personnelles en matière de fiscalité et d'assurances sociales se retrouvent publiées sur Internet.

Parmi les millions d'individus touchés, une personne concernée saisit le tribunal administratif de la ville de Sofia (*Administratibven sad Sofia-grad*, ASSG) alléguant que la NAP a violé son devoir de garantir un niveau de sécurité approprié lors du traitement de ses données personnelles. Elle n'aurait pas mis en place des mesures techniques et organisationnelles (MTO) appropriées, au sens des art. 24 et 32 RGPD. Elle estime de plus avoir subi un préjudice moral, sous la forme d'inquiétudes et de craintes liées à une éventuelle future utilisation abusive de ses données personnelles rendues publiques.

L'ASSG rejette le recours affirmant que la diffusion des données n'est pas imputable à la NAP, qu'il revient à la recourante de prouver le caractère inapproprié des MTO adoptées et qu'aucun préjudice moral indemnisable ne découle de la situation.

La Cour suprême administrative (*Varhoven administrativen sad*) est saisie d'un pourvoi en cassation. Cette dernière saisit la CJUE et lui pose six questions préjudicielles visant l'interprétation du RGPD.

1. Les mesures techniques et organisationnelles sont-elles automatiquement inappropriées en cas de violation de données ?

Le responsable du traitement possède une certaine marge de manœuvre dans le choix des MTO, dans le cadre des critères établis aux art. 24 et 32 RGPD. Plusieurs critères doivent être pris en compte et une balance entre les intérêts de la personne concernée et les intérêts du responsable du traitement doit être faite.

En particulier, le critère de l'avancée technologique prévu à l'art. 32 par. 1 RGPD indique que le responsable de traitement n'est pas tenu d'aller au-delà de ce qui est raisonnablement possible au moment de l'adoption des MTO.

L'objectif du RGPD n'est en effet pas d'exiger le risque « zéro ». Un tel niveau serait impossible à atteindre au vu de l'évolution constante des outils des cybercriminels. De même, le caractère approprié des MTO peut évoluer dans le temps.

La mention de mesures permettant le rétablissement de la disponibilité ou de l'accès des données en cas de violation de l'art. 32 par. 1 let. c RGPD réaffirme que le législateur envisage la possibilité d'une violation, sans pour autant que celle-ci ne remette en cause le caractère approprié des MTO mises en place par le responsable de traitement. Une violation ne saurait ainsi directement supposer que les MTO sont inappropriées.

2. Sur quelles bases le caractère approprié des mesures techniques et organisationnelles doit-il être analysé ?

Une approche *in concreto* est préconisée par l'avocat général. En effet, l'analyse doit porter sur le contenu des mesures, sur leur application ainsi que sur leur effectivité.

Le contenu des mesures fait référence à ce qui est inclus ou prévu dans les mesures en termes de politiques, règles, procédures ou dispositifs. Leur application concerne la manière dont les mesures sont mises en œuvre dans la pratique. Il est important d'examiner si les mesures sont effectivement mises en place conformément à ce qui a été défini et si elles sont appliquées de manière cohérente. Finalement, en ce qui concerne leur effectivité, ce critère se réfère aux résultats et à l'efficacité réelle des mesures mises en place. Il est nécessaire de déterminer si les mesures atteignent les objectifs fixés, s'ils sont efficaces pour prévenir les problèmes de sécurité.

3. Sur qui repose le fardeau de la preuve du caractère approprié des mesures techniques et organisationnelles ?

Pour répondre à cette question, il faut opposer le principe d'*accountability* (terme traduit en

« responsabilité » dans le texte officiel du RGPD, qui cependant ne permet pas, à mon sens, d'englober la signification donnée en anglais) et la charge de la preuve de celui ou celle qui intente une action en réparation sur la base de l'art. 82 RGPD.

En effet, sur la base de l'art. 82 RGPD, la requérante doit pouvoir prouver qu'une violation du règlement a eu lieu, qu'un préjudice ait été subi et qu'un lien de causalité existe entre les deux. L'avocat général précise cependant que la personne concernée n'est pas tenue de démontrer le caractère approprié des MTO pour qu'une violation puisse être retenue. En effet, le responsable de traitement est plus à même d'apporter des preuves sur le caractère approprié des MTO qu'il a mis en place. Cela s'explique notamment par ses connaissances techniques et d'éventuels intérêts prépondérants à ne pas révéler des secrets professionnels si le fardeau était inversé en faveur de la requérante.

De plus, avec le RGPD, l'intention du législateur européen était précisément de consolider les droits des personnes concernées, ce qui serait mis à mal si le fardeau de la preuve reposait uniquement sur la personne atteinte dans sa personnalité.

4. Une expertise judiciaire suffit-elle comme moyen de preuve ?

La question n'étant pas réglée par le RGPD, il faut s'en remettre au principe de l'autonomie procédurale des États membres pour le choix des moyens de preuve.

Dans ce cadre, les principes d'équivalence et d'effectivité doivent être respectés. Ceux-ci requièrent respectivement le maintien d'un même niveau de protection équivalent à celui prévu au niveau national et le fait de ne pas entraver l'exécution des droits conférés par le droit communautaire.

5. La responsabilité peut-elle être imputée au responsable de traitement lorsque la personne à l'origine de la violation de données n'est pas un employé ?

La NAP affirme qu'aucune responsabilité ne peut lui être imputée, car la personne à l'origine de la publication des données sur Internet n'est pas une personne qu'elle emploie.

Le RGPD ne prévoyant pas d'exonération automatique à ce sujet ni de conditions y relatives, le fardeau de la preuve est renversé. Il revient au responsable de traitement de fournir la preuve libératoire en établissant que le dommage ne peut lui être imputable. De plus, le terme « nullement » utilisé à l'art. 82 par. 3 RGPD suppose un niveau de preuve élevé.

Le contrôle exercé ou non sur la personne à l'origine de la violation ne permet pas d'exclure la responsabilité du responsable de traitement. En effet, la violation pourrait être imputée au responsable de traitement lors d'une négligence de sa part, notamment si les MTO mises en place sont insuffisantes.

6. La crainte d'une utilisation abusive future constitue-t-elle un préjudice moral donnant droit à réparation ?

La réparation du dommage tel que prévu à l'art. 82 RGPD vise le rétablissement de la situation juridique négativement impactée par la violation. Le dommage n'étant pas défini, une interprétation large permet d'inclure le dommage moral (cf. https://swissprivacy.law/181/).

Une distinction est faite ici entre un inconvénient résultant du non-respect de la loi par le responsable de traitement et un préjudice moral réel. L'avocat général est d'avis qu'il revient aux juridictions nationales de déterminer la limite entre les deux.

Un « inconvénient » ne donne pas de droit à réparation en raison de sa faible importance et vise des cas dans lesquels la personne concernée ressent un désagrément ou une réaction négative face à une violation du droit, sans pour autant constituer un préjudice réparable.

Un « préjudice moral réel » est quant à lui indemnisable, dans la mesure où des éléments concrets permettent de démontrer un préjudice émotionnel réel et certain pour la personne concernée. À ce titre, on prend notamment en compte les effets sur l'intimité physique et psychique, la vie relationnelle de la personne concernée, la nature des données concernées et l'importance de celles-ci sur la vie de la personne concernée. La perception de la société face à des violations de données personnelles peut également constituer un indice permettant de déterminer si un préjudice a été subi.

Conclusion

Il ressort des conclusions de l'avocat général que les MTO ne peuvent pas garantir un niveau de protection absolu empêchant toute violation de données personnelles.

En pratique, des normes internationales telles que les « ISO » peuvent être utilisées pour démontrer le caractère approprié des MTO. Ces normes fournissent des exigences et des lignes directrices, notamment sur la mise en place de système de gestion de la sécurité de l'information (ISO 27001) ou sur l'établissement de mesures de sécurité des informations (ISO 27002).

Pour se conformer au principe d'*accountability,* il est recommandé pour les responsables du traitement de recenser les mesures mises en place. Dans ce sens, formaliser les procédures à suivre en cas de violation de données permet de fournir une preuve additionnelle du niveau approprié des MTO.

Le concept d'*accountability* est certainement l'un des plus importants introduits par le RGPD. Il s'agit non seulement de dire que le responsable du traitement prend des mesures appropriées, mais également d'être en mesure de prouver qu'il les met en application. L'*accountability* est donc bénéfique pour le responsable du traitement, en particulier dans une affaire comme celle-ci.

Proposition de citation : Charlotte Beck, Faute présumée du responsable de traitement en cas de cyberattaque, 31 mai 2023 *in* www.swissprivacy.law/230