Scraping en masse : la Cour fédérale allemande admet le préjudice indemnisable

Mallorie Ashton-Lomax, le 13 mai 2025

Le *Bundesgerichtshof* (BGH) juge que la simple perte de contrôle sur ses données personnelles constitue un préjudice immatériel indemnisable au sens de l'art. 82 par. 1 RGPD. À la suite de la fuite massive de données de 533 millions d'utilisateurs de Facebook, le BGH estime que le requérant n'a pas à prouver de conséquences concrètes pour obtenir la réparation du dommage causé.

Arrêt de la Cour fédérale de justice allemande (Bundesgerichtshof, BGH), Urt. v. 18. 11. 2024 – VI ZR 10/24

Un résident allemand dispose d'un compte Facebook sur lequel certaines données personnelles (nom, sexe, lieu de travail) sont visibles, tandis que son numéro de téléphone mobile est paramétré comme « privé ». La fonctionnalité « contact-import », activée par défaut, permet à tout utilisateur du réseau social de retrouver son profil en saisissant son numéro de téléphone, alors même que ce numéro n'est pas rendu public dans les paramètres de confidentialités. De janvier 2018 à septembre 2019, des tiers se sont servis de cette fonctionnalité pour effectuer un *scraping* à grande échelle, générant des numéros de téléphone aléatoires (y compris celui du requérant) afin de les associer à des profils et d'en extraire les informations correspondantes. Au total, les données personnelles d'environ 533 millions d'utilisateurs ont été diffusées en accès libre sur internet en avril 2021, parmi lesquelles figuraient le numéro de téléphone du requérant, son nom complet, sa profession et son identifiant sur le réseau social.

Le requérant fait valoir que cette diffusion lui a fait perdre le contrôle de ses données personnelles et l'expose à des risques d'escroquerie et de phishing. Il réclame la réparation de son préjudice immatériel, la reconnaissance d'une responsabilité pour tout dommage futur, ainsi que l'interdiction de toute utilisation de son numéro en l'absence de son consentement explicite.

Le *Landgericht Bonn* fait partiellement droit à la demande du requérant en lui accordant EUR 250.- à titre de dommages et intérêts pour le préjudice immatériel subi. En appel, l'*Oberlandesgericht Köln* annule cette décision. Il juge les demandes irrecevables ou infon-

dées, faute d'intérêt à agir ou de précision, et considère que le requérant ne prouve aucun préjudice immatériel concret. La Cour d'appel considère en effet que la perte de contrôle invoquée n'est pas démontrée, les risques évoqués ne sont ni étayés ni indemnisables, et l'engagement d'un avocat n'est pas justifié.

Le requérant introduit un recours auprès du *Bundesgerichtshof* (BGH). Il conclut à la reconnaissance de son droit à réparation pour préjudice immatériel au titre de l'art. 82 par. 1 RGPD (conclusion 1), à la constatation de la responsabilité de la défenderesse (Facebook) pour tout dommage futur lié à la fuite de ses données (conclusion 2), à l'interdiction d'accès à ses données via l'outil d'importation de contacts (conclusion 3a), à l'interdiction de toute utilisation non autorisée de son numéro de téléphone (conclusion 3b), à l'obtention d'informations sur l'usage de ses données (conclusion 4), ainsi qu'au remboursement des frais d'avocat engagés avant le procès (conclusion 5).

Réparation pour préjudice immatériel

Selon la jurisprudence de la CJUE (voir www.swissprivacy.law/293/), le droit à réparation prévu par l'art. 82 par. 1 RGPD repose sur trois conditions cumulatives : une violation du RGPD, l'existence d'un préjudice (matériel ou immatériel), et un lien de causalité entre le préjudice et la violation. Le requérant n'a pas à prouver une faute de la défenderesse, car le Règlement prévoit une responsabilité pour faute présumée. Il revient donc au responsable du traitement d'apporter la preuve qu'il n'est pas à l'origine du dommage (art. 82 par. 3 RGPD).

S'agissant de la violation du RGPD, le BGH considère qu'elle peut être présumée. En effet et même si l'*Oberlandesgericht Köln* n'a pas tranché ce point, le *scraping* repose sur un traitement de données au sens du RGPD (notamment : stockage, mise à disposition, interconnexion). Or, la configuration par défaut qui permet la recherche universelle via numéro de téléphone contrevient aux principes de minimisation des données et de protection des données par défaut (art. 5 et 25 RGPD).

En ce qui concerne le préjudice immatériel, le simple fait de perdre le contrôle sur ses données personnelles constitue déjà un préjudice au sens de l'art. 82 RGPD, même sans conséquences supplémentaires telles que des suites négatives psychologiques ou financières (CJUE, 4 octobre 2024, C-200/23 Agentsia po vpisvaniyata). En l'espèce, le requérant démontre que des tiers ont rendu public et associé son numéro de téléphone à d'autres données personnelles à la suite du *scraping*. Les tiers impliqués ont ainsi pu accéder à ses données personnelles même si ce dernier avait choisi le paramètre « privé » de confidentialité pour son compte Facebook. Le requérant explicite également les inquiétudes vécues et

les précautions supplémentaires prises suite à cet événement. La perte de contrôle sur ses données personnelles suffit donc à établir un préjudice immatériel réparable.

Le BGH confirme le lien de causalité. En effet, la Cour estime que c'est la configuration par défaut du réseau social qui a permis le *scraping* et la diffusion non souhaitée des données du requérant. Cette faille technique et organisationnelle imputable à la défenderesse est à l'origine directe du préjudice subi (art. 25 et 32 RGPD).

Le BGH relève finalement dans un *obiter dictum* que l'*Oberlandesgericht Köln*, qui a justifié l'atteinte par le consentement donné par l'utilisateur, aurait dû examiner précisément sa validité.

Le BGH reconnaît ainsi le préjudice immatériel du requérant.

Constatation de la responsabilité de Facebook

Le BGH examine ensuite l'injonction du requérant en relation à la constatation de la responsabilité du réseau social pour des dommages futurs résultant de la violation des droits du requérant. Les juges admettent la seule possibilité d'un préjudice futur, sans exiger une forte probabilité de répétition de l'acte. Ils motivent leur décision par la violation du droit fondamental du requérant, en l'occurrence son droit à l'autodétermination informationnelle (art. 2 par. 1 Constitution fédérale allemande). En l'espèce, la publication et présence continue de données personnelles du requérant sur Internet implique un risque persistant d'utilisation de celles-ci à des fins frauduleuses. Ce risque, combiné à la perte de contrôle déjà subie par le requérant, suffit à justifier son intérêt à faire constater la responsabilité de Facebook pour tout dommage ultérieur non encore prévisible.

Injonction d'interdiction d'accès aux données

Le BGH examine ensuite la conclusion par laquelle le requérant entend interdire à Facebook de rendre ses données accessibles à des tiers non autorisés via l'outil d'importation de contacts, sans mesures de sécurité appropriées. Le BGH estime que la formulation de cette conclusion est trop imprécise. En effet, les termes utilisés, tels que « tiers non autorisés » (*unbefugten Dritten*) ou « mesures de sécurité conformes à l'état de la technique » (*nach dem Stand der Technik möglichen Sicherheitsmaßnahmen*), ne permettent pas de cerner clairement la portée de l'interdiction sollicitée. Un tel manque de détermination contrevient aux exigences procédurales allemandes, dès lors que le dispositif d'un jugement doit être directement exécutoire sans générer d'incertitude ou de litige ultérieur quant à son interprétation.

Le BGH rejette le recours sur ce point pour défaut de précision du requérant.

Injonction d'interdiction d'utilisation non autorisée du numéro de téléphone

Le requérant sollicite en outre l'interdiction de toute utilisation de son numéro de téléphone fondée sur son consentement. Celui-ci avance que son consentement à l'utilisation de ses données a été obtenu au moyen d'informations incomplètes et peu claires. Contrairement à l'avis de l'*Oberlandesgericht Köln*, le BGH considère cette demande comme recevable, car suffisamment précise. La demande vise en effet à empêcher tout traitement de la donnée reposant sur un consentement exprimé sans information transparente sur l'utilisation des données. Cela s'applique notamment au fait que la fonction d'importation de contacts permettait au réseau social, malgré le paramètre « privé » choisi par le requérant, d'utiliser son numéro. Le *Bundesgerichtshof* relève en outre que le requérant conserve un intérêt à agir, même s'il peut théoriquement supprimer sa donnée lui-même. Le BGH considère que ce dernier ne peut être tenu de renoncer à l'usage légitime de sa donnée (notamment pour la double authentification) pour se prémunir d'un traitement illicite par Facebook. La question du consentement éclairé doit être examinée au regard des exigences fixées par la CJUE, notamment en matière de transparence et de validité de l'accord au sens de l'art. 4 par 11, et de l'art. 7 par. 2 du RGPD (voir CJUE, 1er octobre 2019, C-673/17 planet49 ; www.swissprivacy.law/244/).

Demande d'information sur l'usage des données personnelles du requérant

Le requérant reproche également à la défenderesse de ne pas lui avoir précisé quels tiers avaient eu accès à ses données lors du *scraping*. Le BGH relève que, le 23 août 2021, Facebook avait déjà informé le requérant par écrit de toutes les données en sa possession le concernant. Quant aux tiers ayant accédé aux données, leur identité est inconnue, ce qui rend impossible toute reddition d'information supplémentaire par le réseau social. Conformément à la jurisprudence de la CJUE, le droit d'accès garanti par l'art. 15 par. 1 let. c RGPD peut être limité lorsque le responsable du traitement ignore l'identité des destinataires (voir www.swissprivacy.law/216/). En outre, le BGH rappelle que le droit à la protection des données n'est pas illimité. Il s'agit de procéder à une pesée d'intérêts avec d'autres droits dans le respect du principe de proportionnalité, conformément au consid. 4 du RGPD. Le BGH ne fait ainsi pas suite à la conclusion du demandeur.

Renvoi de la cause à l'*Oberlandesgericht Köln* et considérations finales

Le BGH casse la décision de l'*Oberlandesgericht Köln* sans statuer elle-même sur l'existence

ou le montant d'un droit à réparation, dès lors où les faits ne sont pas suffisamment établis par l'instance précédente, et renvoie l'affaire à l'*Oberlandesgericht Köln* pour un nouveau jugement dans le sens de ses considérations en droit.

Le BGH invite l'*Oberlandesgericht Köln* à examiner si la configuration par défaut de la fonction de recherche, permettant à tout utilisateur de retrouver un profil via un numéro de téléphone, contrevient au principe de minimisation des données et à l'obligation de prévoir des paramètres respectueux de la vie privée dès la conception, conformément aux art. 5 par. 1 let. b et c, ainsi qu'à l'art. 25 par. 2 RGPD. Elle rappelle que l'accès aux données doit être limité à un cercle déterminé de personnes et que les utilisateurs modifient rarement les paramètres par défaut, ce qui impose une conception protectrice dès l'origine (*privacy by design*). L'instance précédente devra également vérifier si la défenderesse pouvait valablement se prévaloir du consentement du demandeur pour justifier le traitement de son numéro de téléphone. S'agissant de la réparation, le BGH précise que son évaluation relève du droit national selon le principe d'autonomie procédurale (en l'espèce, l'art. 287 ZPO/DE), mais doit assurer une compensation effective, sans fonction punitive, conformément à la jurisprudence de la CJUE (voir CJUE, 20 juin 2024, C-590/22 PS GbR ; www.swissprivacy.law/293/). Le juge ne peut tenir compte ni de la gravité du manquement ni du nombre de violations pour majorer l'indemnité, qui doit uniquement compenser le préjudice subi. La seule perte de contrôle sur les données peut justifier une réparation, mais d'un montant modéré, et dont l'évaluation doit respecter le principe d'effectivité du droit européen.

Conclusion

La décision du BGH s'inscrit dans la même affaire de *scraping* ayant conduit, côté irlandais, la Data Protection Commission (DPC) à condamner Meta (Facebook) le 25 novembre 2022 pour avoir laissé accessibles, par défaut, les données de 533 millions d'utilisateurs. La DPC a jugé que ces paramètres initiaux violaient les principes de sécurité et de minimisation, tout comme le souligne le *Bundesgerichtshof* lorsqu'il invite l'*Oberlandesgericht Köln* à vérifier la conformité de la fonction de recherche par numéro. Même si une procédure individuelle, lourde en coûts et en temps, peut ne pas sembler rentable pour les utilisateurs concernés, l'interprétation large faite du préjudice immatériel dans la décision du BGH ouvre la voie aux avocats allemands spécialisés dans la défense des consommateurs et favorise le recours aux actions collectives (cf. art. 80 par. 1 RGPD).

À l'échelle internationale, les juridictions apprécient toutefois différemment la question du *scraping* : en avril 2022, la Cour d'appel du neuvième circuit de Californie a, par exemple,

autorisé la société hiQ Labs à collecter automatiquement les données publiques sur LinkedIn en se fondant notamment sur la nécessité pour hiQ afin d'être économiquement viable et sur l'absence d'attente de confidentialité pour des profils déjà librement accessibles en ligne (voir www.swissprivacy.law/150/).

Dans un contexte où ces pratiques se multiplient, cette décision met en évidence la nécessité de respecter certains principes fondamentaux du RGPD, dont les principes de minimisation et de transparence du traitement. Dans son opinion du 17 décembre 2024, le Comité européen de la protection des données (EDPB) rappelle par ailleurs que le simple fait qu'une donnée soit librement accessible ne signifie pas que la personne concernée ait décidé de la rendre publique. Il ne faudrait donc pas considérer que le responsable de traitement soit libéré de ses obligations découlant du RGPD à cet égard.

En Suisse, le PFPDT et neuf autres autorités de protection des données ont publié, le 24 août 2023, une déclaration commune sur le *data scraping* et la protection des données. Cette déclaration souligne que la loi protège toujours les informations personnelles, même lorsqu'elles sont accessibles au public. Les plateformes doivent donc assumer leur responsabilité en matière de sécurisation des données, dès lors où le *scraping* peut sérieusement compromettre la confidentialité et provoquer des atteintes à la sécurité. Les autorités encouragent ainsi les réseaux sociaux à adopter des mesures concrètes pour limiter ces risques et enjoignent également les utilisateurs à ajuster leurs paramètres de protection afin de maîtriser la diffusion de leurs informations sur internet.

Proposition de citation : Mallorie Ashton-Lomax, Scraping en masse : la Cour fédérale allemande admet le préjudice indemnisable, 13 mai 2025 *in* www.swissprivacy.law/351