# CAPTCHA : une mesure de sécurité suffisante ?

Pauline Meyer, le 17 février 2023

L'utilisation d'un CAPTCHA et de restrictions de transmission ainsi que l'engagement d'une équipe de professionnels par un réseau social ne sont pas des mesures appropriées pour éviter le *web scraping* automatisé.

Landgericht Paderborn, 3. Zivilkammer, Urteil vom 19.12.2022, 3 O 99/22

Un réseau social permet à ses utilisateurs de communiquer en partageant notamment des photos et informations privées par l'intermédiaire de son site web ou de son application mobile. Lors de l'inscription, les utilisateurs fournissent au réseau social leur nom, leur sexe et leur numéro d'identification (ID) d'utilisateur. Ces informations font partie intégrante du profil utilisateur et sont visibles publiquement par défaut. En revanche, la saisie du numéro de téléphone n'est pas obligatoire.

Le réseau social permet aux utilisateurs de comparer par un outil d'importation de contacts (*Contact-Import-Tool*, CIT) les contacts enregistrés au sein de leur répertoire téléphonique avec les utilisateurs du réseau social afin de pouvoir les ajouter comme amis. Cette démarche est possible que l'autre utilisateur ait rendu son numéro de téléphone public après la « sélection du groupe cible » ou non.

Entre 2018 et 2019, le réseau social a été le théâtre d'un *web scraping* automatisé (pour une définition du *web scraping*, cf. www.swissprivacy.law/150/). Ce procédé n'est pas effectué directement par le biais du réseau social, qui interdit par ailleurs cette pratique dans ses conditions d'utilisation. Au contraire, les *scrapers* parviennent à leurs fins par le biais du CIT, plus précisément en téléchargeant des contacts contenant des numéros de téléphone potentiels d'utilisateurs à l'aide de l'outil puis en déterminant si ces numéros sont associés à un compte sur le réseau social. Si c'est le cas, ils copient les informations publiques du profil et les corrèlent avec le numéro de téléphone obtenu.

Faisant suite à cet incident, la troisième chambre civile du *Landgericht* Paderborn est saisie et rend sa décision le 19 décembre 2022, condamnant le réseau social. Elle admet principalement une violation du principe de sécurité des données (art. 5 par. 1 let. f RGPD) et des obligations légales en découlant (art. 32 à 34 RGPD).

L'art. 32 RGPD concrétise le principe de sécurité en imposant aux responsables du traitement de mettre en œuvre les mesures techniques et organisationnelles permettant de garantir un niveau de sécurité dans les traitements de données qu'ils effectuent. Cette obligation sert à protéger les données personnelles notamment contre les accès non autorisés.

En vertu de l'art. 32 par. 1 RGPD, le responsable du traitement mettant ces mesures en place doit tenir compte de divers éléments dont le risque causé par le traitement pour les droits fondamentaux des personnes concernées. La probabilité et la gravité de ce risque sont déterminées en fonction de la nature, de la portée, du contexte et des finalités du traitement (consid. 76 RGPD). La chambre du *Landgericht* considère qu'en l'espèce le risque est élevé, dès lors que le risque que les données soient publiées est élevé et qu'il en découle un risque d'usurpation d'identité, de *phishing* ou de manœuvres similaires et, par conséquent, de dommages matériels et immatériels.

Pour être adaptées aux risques, les mesures doivent être efficaces proportionnellement à l'ampleur du risque et au degré de probabilité de survenance d'un dommage. Il en résulte que plus les dommages sont imminents et élevés, plus les mesures doivent répondre à un niveau élevé d'exigences.

Pour faire face au risque et au moment de l'incident le réseau social utilise un CAPTCHA. Il émet également des restrictions de transmission réduisant le nombre de demandes de certaines données qui peuvent être faites par utilisateur ou à partir d'une adresse IP donnée pendant une période donnée. Il bénéficie finalement aussi des compétences d'une équipe d'analystes et d'ingénieurs.

Compte tenu du risque élevé, la chambre du *Landgericht* estime que les mesures en place au moment de l'incident ne sont pas suffisantes par rapport au risque engendré par un accès non autorisé par *web scraping* automatisé. Tout d'abord, les CAPTCHAs devraient être utilisés dans des situations où le risque de tels incidents est moins élevé. Ensuite, les *scrapers* ont la possibilité de contourner les restrictions de transmission. Finalement, les équipes de professionnels sont principalement actives une fois un évènement détecté et leur rôle préventif est trop limité pour permettre d'éviter ce type d'incidents.

Le risque d'atteinte aux droits et libertés des personnes concernées étant considéré comme élevé, la chambre du *Landgericht* conclut également à une violation de l'obligation de notifier l'autorité de contrôle ainsi qu'une violation de l'obligation d'informer les personnes concernées (art. 33 et 34 RGPD).

En parallèle, la chambre admet d'autres violations dont une violation de l'art. 13 par. 1 let. c RGPD, dans la mesure où, bien que le réseau social semble informer suffisamment sur la collecte du numéro de téléphone et les paramètres y étant liés, tel n'est pas le cas pour le CIT. En utilisant cet outil, le réseau social permet à un utilisateur de comparer ses contacts téléphoniques avec des profils d'utilisateurs enregistrés sur le réseau social. En saisissant n'importe quel numéro, l'utilisateur peut donc ajouter en tant qu'ami le profil d'utilisateur associé à celui-ci, sans que le réseau social ne fournisse d'information à ce sujet.

En droit suisse, l'on pourrait considérer comme l'a fait la chambre du *Landgericht* que ce cas de *web scraping*, effectué à partir de données non librement accessibles, constitue une violation de la sécurité des données au sens de l'art. 5 let. h nLPD. L'utilisation par les *scrapers* du CIT pour aspirer des données constitue effectivement un accès non autorisé dans la mesure où les personnes ayant pu avoir accès aux informations en croisant les informations avec les numéros grâce au CIT n'y sont pas habilitées. Partant, est-ce qu'une violation du principe de sécurité (art. 8 nLPD) serait à déplorer aussi en droit suisse dans un cas similaire ?

L'art. 8 al. 1 nLPD requiert des responsables du traitement, de la même manière qu'en droit européen, la mise en place de mesures appropriées au risque (art. 1 ss OPDo). Théoriquement, le raisonnement de la chambre du *Landgericht* pourrait selon nous être soutenu de façon analogue en droit suisse, à savoir que les mesures doivent être plus élevées que ce qui est mis en place dans l'affaire susmentionnée. Une telle réflexion s'explique par les risques engendrés par la possible publication des données, à l'instar des risques d'usurpation d'identité ou de *phishing*, qui peuvent selon nous constituer un risque élevé pour la personnalité et les droits fondamentaux des personnes. Cela étant, il n'est pas certain que le PFPDT et nos autorités judiciaires partagent ce raisonnement.

Concrètement, quelles mesures pourraient donc être appropriées ? Le droit suisse n'est pas plus précis que le RGPD à cet égard. À l'aune du RGPD, la chambre du *Landgericht* suggère des mesures telles que la demande d'informations ou l'ajout de variables supplémentaires lors du croisement de contacts avec les utilisateurs du réseau social. Le réseau social pourrait par exemple requérir, en plus du numéro, un nom ou un prénom. Une telle pratique rendrait plus difficile l'accès automatisé aux données personnelles et permettrait probablement plus facilement une alerte de l'équipe de sécurité informatique.

_swissprivacy.law

Proposition de citation : Pauline MEYER, CAPTCHA : une mesure de sécurité suffisante ?, 17 février 2023 *in* www.swissprivacy.law/201