Droit d'accès : quelles limites pour l'ancien employé ?

Livio di Tria, le 14 mars 2021

L'Autorité belge de protection des données a confirmé le refus d'une entreprise de donner suite à une demande de droit d'accès formulée par un ancien employé et concernant, entres autres, les logs IT et les courriels le concernant. L'Autorité estime qu'une telle communication représenterait pour l'entreprise une charge de travail disproportionnée et violerait son droit à la protection du secret d'affaire.

Autorité belge de protection des données, décision de la Chambre contentieuse 15/2021 du 9 février 2021

L'affaire oppose une société belge active dans le secteur de la consultation informatique face à l'un de ses anciens employés. Ce dernier y a travaillé de 2008 à 2019. Les dernières années de leur relation contractuelle de travail étaient conflictuelles. À ce titre, l'employé était régulièrement absent à partir d'octobre 2015. Une procédure prud'hommale a même été introduite par la société en 2017. La procédure s'est soldée en juin 2018 par un échec, forçant la société à réintégrer son employé en son sein. Leur relation contractuelle s'est toutefois éteinte en janvier 2019, après la conclusion d'une transaction privée.

Quelques jours après le jugement prud'hommale, l'employé a exercé son droit d'accès contre la société (art. 15 RGPD). Il a exigé de la société la communication de toutes les données personnelles enregistrées à son sujet, et spécifiquement :

- les annotations ou commentaires faisant partie de son dossier RH ;
- les logs IT le concernant ;
- les évaluations le concernant ;
- la copie de ses courriels contenus dans sa boîte électronique (qu'il en soit l'expéditeur ou le destinataire) ;
- les photos sur lesquelles il pouvait être identifié.

Le 19 septembre 2018, la société a donné suite à la requête du plaignant en lui fournissant la cartographie de ses données personnelles, leur contenu, les CV le concernant ainsi que les photos d'identité enregistrées. Insatisfait par la réponse, l'employé a interpellé la société le 24 septembre 2018 pour qu'elle lui remette encore les documents spécifiquement souhaités.

La société estimant que l'affaire était close, l'employé a introduit une réclamation auprès de l'autorité conformément à l'art. 77 RGPD, ayant débouché sur une décision l'Autorité belge de protection des données (ci-après : l'Autorité).

À titre liminaire, nous mentionnons que l'Autorité reconnaît que le droit d'accès couvre nécessairement le droit de copie, en ce qu'il en est un prérequis. Elle insiste également au long de son argumentation sur l'importance du droit d'accès, qui est pour elle un des fondements du droit à la protection des données. Il constitue en effet la porte d'entrée qui permet l'exercice des autres droits que le RGPD confère à la personne concernée. Ainsi, toute limitation au droit d'accès doit être interprétée de façon restrictive.

En ce qui concerne les points évoqués par l'employé, nous nous bornerons à limiter notre analyse aux annotations, aux logs IT ainsi qu'à la copie des courriels.

Annotations dans le dossier RH

La société refuse d'octroyer au plaignant l'accès aux annotations faisant partie de son dossier RH en vertu de l'art. 15 par. 4 RGPD. Selon la société, l'accès à ces données violerait la protection des données des anciens supérieurs hiérarchiques du plaignant, auteurs de ces annotations ou commentaires. L'Autorité n'est pas convaincue par cette argumentation.

Premièrement, elle souligne que, conformément à l'arrêt Nowak de la Cour de justice de l'Union européenne, la notion de données personnelles englobe les cas d'évaluations qui peuvent refléter un avis ou une appréciation concernant une personne, notamment en lien sur ses performances.

Deuxièmement, l'Autorité insiste sur le fait que la mise en balance du droit à l'obtention d'une copie avec les droits et libertés d'autrui ne peut aboutir automatiquement à l'absence de toute communication d'information, une mesure plus adéquate pouvant être trouvée. En l'espèce, puisque l'art. 15 par. 3 RGPD ne requiert pas qu'une copie du document original soit fournie à la personne concernée, il appartient à la société d'anonymiser le nom ou toute donnée personnelle des auteurs des annotations.

Logs IT

La société refuse ensuite de transmettre au plaignant les logs IT le concernant en raison de la quantité de travail disproportionnée que cela lui demanderait, notamment au vu de l'énorme quantité de données à vérifier.

Nous précisons ici que les logs IT sont des fichiers contenant des données de journalisation. Il s'agit donc d'une mesure technique qui consiste à enregistrer les informations pertinentes (p. ex. date, heure, auteur, motifs, etc.) concernant les événements d'un système informatique (p. ex. accès au système ou à un de ses fichiers, modification d'un fichier, suppression d'un fichier, etc.). Le log IT est donc en quelque sorte le procès-verbal de la journalisation. L'Autorité souligne d'ailleurs l'importance de la journalisation à l'aune du principe de sécurité (art. 5 par. 1 let. f RGPD).

L'Autorité reconnaît qu'il faille trouver un juste équilibre entre l'intérêt de la personne concernée à protéger sa vie privée et la charge que l'obligation représente pour le responsable du traitement. En l'espèce, une fouille systématique des logs IT concernant le plaignant (allant de son entrée en fonction à la cessation de son contrat de travail) représenterait effectivement une charge de travail disproportionnée. En outre, le plaignant n'a pas démontré d'intérêt particulier à sa demande.

Copie des courriels

La société refuse finalement la transmission de copie des courriels dont le plaignant est le destinataire ou l'expéditeur. Selon la société, une telle transmission contreviendrait au secret des correspondances électroniques et ne serait pas nécessaire puisque le plaignant avait, lors de la demande, accès à ses courriels.

L'Autorité n'est pas convaincue par les arguments. D'abord, le secret des correspondances électroniques s'applique uniquement envers les tiers aux communications électroniques concernées, et non pas à une personne partie aux communications. Ensuite, le fait d'avoir accès aux données en question n'exclut pas le droit d'en obtenir une copie. De même, le fait d'avoir connaissance des données traitées ne constitue pas non plus une raison valable pour en refuser l'accès.

En dernier lieu, la société soulève que la transmission des courriels violerait son droit à la protection du secret d'affaire. L'Autorité rappelle tout d'abord l'importance d'analyser une restriction au droit d'accès de façon limitée. En l'espèce, le risque de la violation du secret d'affaires est clairement démontré. En effet, le plaignant occupe une fonction dirigeante au sein de la société, ce qui lui donne accès à de nombreuses informations sensibles sur les affaires de la société. Il s'agit par exemple de l'identité des clients, des montants des commandes ou encore des montants des factures. L'Autorité ajoute toutefois que si le risque n'avait pas été démontré, l'anonymisation des données aurait pu être envisagée.

À toutes fins utiles, nous précisons qu'une solution similaire avait été retenue par le *Berliner Beauftragte für Datenschutz und Informationsfreiheit* dans le cadre d'une affaire assez identique (Rapport d'activités 2019, pp. 119–120). Celle-ci concernait le cas d'un ancien cadre d'une banque qui demandait à son ancien employeur de lui remettre une copie de tous ses courriels. L'Autorité berlinoise avait là aussi retenu l'intérêt de la banque à protéger ses secrets d'affaires, tout en reconnaissant que les courriels envoyés à titre privé devaient être remis au requérant.

Notes

En Europe comme en Suisse, le droit d'accès à ses données personnelles est considéré comme une institution clef de la protection des données. Comme le rappelait l'Autorité belge, il permet à toute personne concernée de savoir si des données la concernant sont traitées et, cas échéant, d'y avoir accès. Cela permet à la personne d'en vérifier le contenu (et *a fortiori* d'en vérifier l'exactitude), tout en s'assurant que les données sont traitées de manière licite. Dans cette optique, le droit d'accès est facile à exercer et ne demande pas de motivation ou de justification.

Bien qu'essentiel, le droit d'accès peut s'avérer être un outil utilisé à mauvais escient. Tel est le cas lorsque le demandeur est uniquement motivé par un sentiment de « représailles » vis-à-vis du responsable du traitement, l'objectif étant là de recourir au droit d'accès comme une « forme de nuisance ». Cette affirmation est particulièrement vraie dans le cadre d'une relation de travail conflictuelle. À l'aune de ces considérations, et avec comme point d'ancrage le droit suisse actuel et futur, nous souhaitons soulever plusieurs aspects de la décision qui suscitent, selon nous, le questionnement.

Premièrement, il nous semble justifié de considérer que le droit d'accès recouvre nécessairement le droit de recevoir copie des documents dans lesquels figurent des données personnelles. Le requérant qui exerce son droit d'accès à un intérêt évident à obtenir une copie des données personnelles, puisque cela lui permet de les consulter n'importe où et n'importe quand, facilitant ainsi une possible comparaison avec d'autres données en sa possession. Si la jurisprudence en la matière reste rare, nous soulignons que le Tribunal fédéral semble toutefois déduire du droit d'accès le droit à recevoir copie (ATF 141 III 119, consid. 7.3).

Ce lien entre droit d'accès et droit de recevoir copie semble connu du législateur fédéral. En effet, lors de la récente révision totale de la LPD, le droit d'accès (art. 25 nLPD) a fait l'objet d'une modification matérielle. Cette dernière porte sur les informations qui devront être communiquées par le responsable du traitement au requérant. Parmi ces informations, le

responsable du traitement devra notamment transmettre « les données personnelles traitées en tant que telles » (art. 25 al. 2 let. b nLPD).

Cette notion a été introduite par la Commission des institutions politiques du Conseil national et appelle à la réflexion. Selon les débats parlementaires (BO 2020 N 150), cette notion a pour objectif de limiter le droit d'accès en excluant que soit transmise « toute la documentation qui peut contenir les données personnelles », acte que le législateur juge disproportionné. Cette expression n'apporte toutefois pas de clarté au problème soulevé par le droit de recevoir copie. Selon nous, même à l'aune du nouveau droit, les documents contenant des données personnelles ne pouvant être extraites ou au prix d'un travail disproportionné devraient continuer à être communiqués. Dans le cas contraire, le droit d'accès se retrouverait vidé de sa substance.

Deuxièmement, il nous semble important de nuancer la décision belge à l'égard des logs IT. Le droit fédéral actuel oblige le responsable du traitement de journaliser les traitements automatisés de données sensibles ou de profils de la personnalité, conformément à l'art. 10 al. 1 OLPD. Le PFPDT peut par ailleurs recommander la journalisation pour d'autres traitements, notamment ceux qui présentent un risque élevé d'atteinte à la vie privée et aux droits des personnes concernées. Selon le commentaire de l'Office fédéral de la justice à l'appui de l'OLPD, tel est le cas notamment lorsque le traitement présente un certain degré de sensibilité, soit en raison du domaine (p. ex. assurances, agences de renseignements), soit en raison de la configuration du système d'informations.

Mesure technique intimement liée à la gestion d'un système informatique, les procès-verbaux de journalisation ne devraient être conservés que durant une année selon l'art. 10 al. 2 OLPD. Ce délai de conservation d'une année est également repris au sein de l'art. 16 al. 1 OPDC. Si la durée d'une année nous semble légèrement courte, le cas belge représente l'autre extrémité puisque le plaignant demandait l'accès à des logs IT remontant aux prémices de la relation de travail, soit 2009. Le principe de proportionnalité exige en effet la suppression des données dès qu'elles ne sont plus nécessaires. Il est regrettable que la décision belge n'aborde pas ce point.

Toujours sur les logs IT, nous déplorons également que l'Autorité belge ne se soit pas penchée sur leur qualification juridique à proprement parler. Sans aucune précision, l'Autorité belge part du principe que les logs IT sont (ou contiennent) des données personnelles. Selon nous, les logs IT sont des mesures techniques qui permettent au responsable du traitement une forme de contrôle s'agissant du système informatique. La vocation des logs IT n'est donc

pas de faire partie du dossier d'un employé, elles constituent toutefois une ressource importante en cas d'audit. Au vu de ce qui précède, les données issues des logs IT ne devraient tomber dans le champ du droit d'accès que si elles sont incorporées au sein d'un dossier dans lequel se trouvent les données personnelles du requérant.

Troisièmement, nous souhaitons aborder la question de la restriction au droit d'accès, spécifiquement dans le cadre d'une relation de travail conflictuelle. Selon nous, deux restrictions peuvent potentiellement être soulevées par l'employeur dans le cadre d'une demande de droit d'accès.

La première restriction pourrait concerner l'abus de droit au sens de l'art. 2 al. 2 CC. Par exemple, une demande de droit d'accès qui ne vise qu'à se procurer des preuves en vue d'une procédure civile est contraire au but de l'art. 25 nLPD et constitue un abus de droit selon l'art. 2 al. 2 CC. Ce cas a d'ailleurs été récemment traité par le Tribunal fédéral (Arrêt 4A_277/2020 du 18 novembre 2020), et déjà résumé (Célian Hirsch, Le droit d'accès abusif, in : www.swissprivacy.law/45).

La seconde restriction concerne l'art. 26 al. 1 let. c nLPD qui prévoit qu'un responsable du traitement peut notamment refuser la communication des renseignements si la demande d'accès est manifestement infondée notamment parce qu'elle poursuit un but contraire à la protection des données ou est manifestement procédurière. Il s'agit d'une nouvelle restriction intégrée lors de la révision totale de la LPD.

L'expression « manifestement procédurière » est empruntée aux règles procédurales, à l'instar des art. 42 al. 7 LTF ou 132 al. 3 CPC. Dans le cadre de ces règles, l'expression « procédurier » s'entend comme le recours qui est introduit par pur esprit de chicane avec comme objectif de tracasser l'adversaire. Cela découle notamment de la multiplication des procédures, de la disproportion évidente entre l'enjeu et les procédés utilisés, voire des propos qui figurent dans le recours.

Un raisonnement similaire doit valoir en ce qui concerne la demande de droit d'accès. En pratique, il arrive souvent qu'un employé qui vient d'être licencié fasse usage de son droit d'accès (lui-même, ou par l'intermédiaire de son avocat). Il est clair que la proximité temporelle entre le licenciement et la demande de droit d'accès peut donner, dans une certaine mesure, un indice sur cet esprit de chicane.

Toutefois, toute restriction au droit d'accès doit s'analyser de manière restrictive. Et une relation conflictuelle de travail n'atteste pas automatiquement, en fait, de la volonté du requé-

rant de faire usage du droit d'accès de manière contraire au but qui est le sien, pas plus qu'elle atteste automatiquement d'un esprit de chicane. L'employeur ne pourrait, selon nous, soulever cette exception que dans les cas particulièrement choquants et dûment avérés.

Dans l'absolu, et au vu des hypothèses susmentionnées, l'employeur aura tout à gagner à ne pas refuser de communiquer les renseignements, mais plutôt d'en différer l'envoi. Charge alors au requérant d'user de son droit d'introduire une action en exécution du droit d'accès auprès du tribunal compétent. À cet égard, la procédure sera désormais exemptée de frais judicaires (art. 113 al. 2 let. g et 114 let. g nCPC) et continuera à se faire sous la forme d'une procédure simplifiée (art. 243 al. 2 let. d CPC, art. 243 al. 2 let. d nCPC).

Proposition de citation : Livio DI TRIA, Droit d'accès : quelles limites pour l'ancien employé ?, 14 mars 2021 *in* www.swissprivacy.law/62

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.