Tribunal fédéral – 4A_83/2020
Ire Cour de droit civil
Arrêt du 16 juillet 2020 (d)

Résumé et commentaire

Proposition de citation :

Sébastien Fanti, Quand l'exercice d'un droit d'accès se transforme en nœud gordien ; commentaire de l'arrêt du Tribunal fédéral 4A_83/2020, Newsletter DroitDuTravail.ch janvier 2021

Newsletter février 2021

Protection de la personnalité, protection des données

Quand l'exercice d'un droit d'accès se transforme en nœud gordien ; commentaire de l'arrêt du Tribunal fédéral 4A_83/2020

Sébastien Fanti, avocat et notaire, préposé à la protection des données et de la transparence du Canton du Valais, CAS Digital Finance Law, Médiateur LSFin

I. Objet de l'arrêt

Cet arrêt, rendu dans le cadre d'un litige de droit du travail et de droit de la protection des données, génère des interrogations plurifactorielles. Dès lors qu'il ne met pas un terme au différend entre les parties, il ne constitue toutefois pas une réponse définitive. Ce nonobstant, il mérite une attention particulière, car la création de bases de données de sécurité privées comporte des risques désormais bien identifiés, notamment en termes d'impossibilité subséquente de travailler dans un secteur particulier.

II. Résumé de l'arrêt

A. Les faits

Un collaborateur engagé par une banque se voit signifier, avant même son entrée en fonction, « l'annulation » de son contrat en raison d'inscriptions le concernant dans une base de données dans laquelle l'établissement bancaire enregistre des informations relatives à la sécurité des personnes[1]. Cette base de données s'intitule « Global Tracking System » (GTS).

Le demandeur d'emploi intente alors une action contre la banque en se fondant sur l'article 328*b* du Code des obligations[2].

---

[1] Cette base de données permet d'opérer un contrôle de sécurité (background check), cf. Préposé fédéral à la protection des données et à la transparence, Explications relatives aux contrôles de sécurité (employés du secteur privé), mars 2015, accessible à cette adresse : https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/arbeitsbereich/explications-relatives-aux-controles-de-securite--employes-du-se.html

[2] L'article 328*b* prévoit que l'employeur ne peut traiter des données concernant le travailleur que dans la mesure où elles portent sur les aptitudes de celui-ci à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail. L'article 328*b* *in fine* renvoie en outre aux dispositions de la Loi fédérale sur la protection des données du 19 juin 1992 (RS 235.1), étant précisé que la portée de ce renvoi est débattue en doctrine

Par jugement du 6 février 2018, le Tribunal du travail de Zurich a ordonné à la banque, sous les sanctions de l'article 292 du Code pénal[3], de fournir au requérant des informations sur son inscription dans la base de données GTS, en particulier de l'informer par écrit du contenu, du but, de l'origine et de l'utilisation de l'inscription, dont copie devait lui être remise.

La banque a fait appel de cette décision auprès de l'Obergericht du canton de Zurich, en concluant à ce que la procédure soit rayée du rôle, car elle était devenue sans objet, tout en déposant une copie de l'inscription litigieuse, l'identité des créateurs des insertions dans la base de données ayant été anonymisée[4]. L'Obergericht du canton de Zurich a, par arrêt du 19 décembre 2018[5], rejeté l'appel et confirmé la décision de première instance au motif que la banque n'avait pas pleinement respecté son obligation de divulgation en présentant des extraits expurgés qui ne permettaient pas de tirer des conclusions concrètes, notamment sur l'origine des données.

Après que le demandeur d'emploi eut requis la banque, les 8 et 16 avril 2019, de lui fournir des informations complètes pour les 22 et 23 avril 2019, cette dernière a contacté les tiers concernés par la divulgation. Deux de ces personnes ont refusé que leur identité soit communiquée et ont saisi, le 18 avril 2019, le Bezirksgericht[6] de Zurich d'une requête de mesures superprovisionnelles, laquelle a été admise. Il a donc été fait interdiction à la banque de fournir au requérant[7] des extraits ou des informations provenant du GTS ou corrélées à celui-ci, informations dont les noms ou autres données personnelles des deux tiers peuvent être inférées.

La banque a alors demandé (le 23 avril 2019), et obtenu du Bezirksgericht de Zurich, qu'il soit sursis à l'exécution du jugement du Tribunal du travail du 6 février 2018 pour la durée de l'interdiction prononcée par le Bezirksgericht de Zurich. Le Tribunal a également jugé que la banque devait informer le demandeur d'emploi tous les trois mois de l'évolution de la procédure divisant la banque et les tiers intéressés. Le demandeur d'emploi a fait appel de cette décision devant l'Obergericht du canton de Zurich[8], puis devant le Tribunal fédéral, sans succès.

L'Obergericht a considéré, après une pondération des intérêts en cause, que surseoir (provisoirement) à l'exécution était légitime, car le Tribunal du travail n'avait pas pris en

---

(cf. pour un exposé des différentes positions, ALEXANDRE GUISAN/CÉLIAN HIRSCH, La surveillance secrète de l'employé, De la protection de données à la procédure pénale, RSJ 115 (2019) N. 23, p. 709 et les références citées).

3 L'article 292 du Code pénal sanctionne l'insoumission à une décision de l'autorité d'une contravention (amende pouvant s'élever à 10'000 francs). Lorsque la décision est adressée à une entreprise, la punissabilité concerne concrètement les membres de sa direction (art. 29 du Code pénal).

4 Ces personnes étaient enregistrées dans le système en qualité de créateurs des entrées litigieuses. Leurs données ont été anonymisées.

5 OGer ZH, LA180010, 19.12.2018 ; accessible à cette adresse : https://www.gerichte-zh.ch/fileadmin/user_upload/entscheide/oeffentlich/LA180010-O7.pdf.

6 Einzelgericht Audienz.

7 Ou à d'autres tiers.

8 OGer ZH, RV 190004, 12.12.2019 ; accessible à cette adresse : https://www.gerichte-zh.ch/fileadmin/user_upload/entscheide/oeffentlich/RV190004-O7.pdf ; pour un commentaire de cet arrêt cantonal ainsi qu'une analyse procédurale, cf. ARNOLD F. RUTSCH, Bundesgericht, I. zivilrechtliche Abteilung, Urteil 4A_83/2020 vom 16. Juli 2020, A. gegen B. AG, vorläufige Einstellung der Vollstreckung, AJP 2020, p. 1634 ss.

considération les droits des tiers lors de sa décision[9]. Il a finalement été relevé qu'en cas d'interdiction définitive de la divulgation des données litigieuses, le demandeur d'emploi aura le droit de recourir[10].

B. Le droit

L'arrêt du Tribunal fédéral est bref. Le recours a été déclaré irrecevable en raison d'une absence de risque de préjudice irréparable et du fait que l'admission du recours ne pouvait conduire à une décision finale immédiate (art. 93 al. 1 let. a et b LTF[11]).

Le Tribunal fédéral n'a pas suivi l'argument selon lequel l'admission du recours engendrerait une décision immédiatement définitive, laquelle permettrait d'économiser du temps et des frais importants en termes de procédure probatoire. Il a retenu qu'il ne ressortait pas des observations du recourant de quelle procédure de preuve spécifique il s'agissait et encore moins de son caractère long et coûteux (art. 93 al. 1 let. b LTF).

S'agissant de la question de l'existence d'un préjudice irréparable (art. 93 al. 1 let. a LT), il a été considéré qu'il ne pouvait se matérialiser du fait que la décision attaquée générait un retard dans l'exécution immédiate de la décision de remise des informations sur l'inscription dans la base de données. Selon la jurisprudence[12], la prolongation de la procédure est un inconvénient de fait qui ne permet pas d'invoquer l'existence d'un tel préjudice. Finalement le grief du recourant relatif à une violation du droit d'être entendu n'a pas plus trouvé grâce aux yeux des juges fédéraux qui ont souligné le fait que celui-ci serait entendu à nouveau dans le cadre de la décision finale sur la suspension de l'exécution.

Il a donc été considéré, en définitive, que les conditions d'un recours contre une décision préjudicielle (art. 93 al. 1 LTF) n'étaient pas remplies. Le recourant doit donc supporter les frais à hauteur de 1'000 francs, de même qu'une indemnité à titre de dépens de 2'500 francs[13].

III. Analyse

La base de données Global Tracking System a fait l'objet de différentes publications dont l'une particulièrement critique sur un blog de référence en matière financière[14]. Son contenu, de même que l'identité de ses auteurs, font l'objet de conjectures et de griefs depuis plusieurs années[15]. En toutes hypothèses, il convient de constater que cette base de données est

---

9 Les juges se sont notamment référés à l'article 341 al. 3 CPC, lequel permet à la partie succombante d'alléguer des faits s'opposant à l'exécution, s'ils se sont produits après la notification de la décision. Les faits postérieurs doivent être des faits susceptibles de modifier la prestation même tranchée, à l'instar de l'extinction, du sursis, de la prescription ou de la péremption (arrêt non publié 4A_43/2017 du 7 mars 2017, considérant 6). De surcroît, les tiers intéressés n'avaient pas été entendus durant la procédure antérieure.

10 En application de l'article 346 CPC.

11 RS 173.110.

12 ATF 144 III 475, consid. 1.2.

13 Il convient de mentionner ces montants en préambule de l'analyse sous chiffre III.

14 Les informations publiées sur ce blog sont régulièrement reprises par les médias ; à titre exemplatif, le possible rapprochement entre l'UBS et le Crédit suisse a été annoncé par ce blog puis repris par l'ensemble de la presse suisse et étrangère.

15 LUKAS HÄSSIG, Inside Paradelplatz, Stasi UBS ? Interne Polizei der Grossbank führt Geheimdatenbank mit heiklen Personendaten – was weiss CEO Ermotti ?, 4 mai 2012, accessible à cette adresse : https://insideparadeplatz.ch/2012/05/04/stasi-ubs/.

activement utilisée, puisqu'il y est fait expressément référence dans au moins une autre décision judiciaire[16].

L'arrêt du Tribunal fédéral n'aborde que superficiellement cette thématique, que ce soit au stade de l'état de fait ou de la subsomption. Cela est dû à la nature du litige à trancher devant la Haute Cour, litige essentiellement procédural. Seules les décisions cantonales zurichoises sont susceptibles d'offrir quelques renseignements à ce sujet.

La consultation de la base de données[17] du Préposé fédéral à la protection des données et à la transparence[18] consacrée aux registres des fichiers déclarés par des personnes privées ou des organes fédéraux n'est pas plus fructueuse. Une déclaration de fichiers est nécessaire[19] lorsqu'une personne privée, respectivement une entreprise traite régulièrement des données sensibles ou des profils de personnalité ou communique régulièrement des données personnelles à des tiers qu'il s'agisse de données sensibles, de profils de personnalité ou d'autres données personnelles. Il va sans dire qu'une banque de données consacrée à la sécurité des personnes entre dans cette catégorie et eût dû être annoncée, la création de profils de personnalité[20] étant une évidence[21]. La banque a toutefois fait usage de l'article 11*a* al. 5 let. e LPD, selon lequel le responsable du traitement peut désigner un conseiller à la protection des données qui est chargé de tenir un inventaire des traitements et de surveiller que, du point de vue interne, les conditions-cadres de la protection des données sont respectées.

Si les contrôles de sécurité sont parfaitement compréhensibles et légitimes dans un domaine d'activité comme le domaine financier, il convient de relever que ces contrôles sont soumis à des garde-fous. Ces contrôles doivent, dans le secteur privé, respecter principalement l'article 328*b* CO et la LPD[22]. En termes de protection des données, le Préposé fédéral à la

---

16 Arrêt non-publié du Tribunal fédéral 8C_846/2018 du 28 mars 2019 considérant 4.2.

17 La base de données est accessible à cette adresse : https://www.datareg.admin.ch/search/SearchSimple.aspx.

18 Abrégé ci-après PFPDT.

19 En vertu de l'article 11*a* al. 3 LPD et des articles 3 et 4 de l'Ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993 (RS 235.11 ; abrégée ci-après OLPD) ; pour de plus amples informations sur l'obligation de déclaration, cf. la fiche informative du PFPDT intitulée « La déclaration des fichiers en bref », accessible à cette adresse : https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/entreprises/declaration-des-fichiers.html

20 Un profil de personnalité est quant à lui un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique (art. 3 let. d LPD). Le profil de personnalité peut soit révéler une image complète de la personne, soit une image partielle, mais qui porte sur ses caractéristiques essentielles (à titre exemplatif et non exhaustif : profil établi par un gestionnaire de fortune, expertise graphologique ou psychologique, test de personnalité, dossier financier complet, ensemble des références de lecture dans une bibliothèque, profil de navigation sur Internet, relevé des transactions effectuées par carte de crédit, blog personnel rédigé de manière d'un journal intime, dossier de candidature d'employé avec curriculum vitae et certificats). Les profils de la personnalité ne concernent que les personnes physiques, à l'exclusion des personnes morales.

21 Pour une analyse du droit d'accès aux données détenues par une entreprise de sécurité, cf. LIVIO DI TRIA/ KASTRIOT LUBISHTANI, Etude empirique du droit d'accès à ses données personnelles, in : Sylvain Métille (édit.), Le droit d'accès, Berne 2021, pp. 52 ss.

22 Dans le secteur public, il existe des normes particulières à l'instar de l'Ordonnance sur les contrôles de sécurité relatifs aux personnes du 4 mars 2011 (OSCP ; RS 120.4), cf. notamment OLIVIER BLEICKER, Contrôles de sécurité relatifs aux personnes, *in* : Sécurité & Droit 3/2015, p. 157 ; pour un exemple de litige relatif au

protection des données et à la transparence rappelle quelles sont les règles à respecter sur son site internet[23]. L'employeur doit informer[24] le candidat au poste de travail du fait qu'un contrôle de sécurité va intervenir et l'orienter de manière précise sur le but du contrôle, son ampleur, la durée de conservation des données, et l'identité de la personne qui va opérer ce contrôle[25]. Il doit motiver le contrôle, qui ne peut dès lors s'opérer de manière secrète. Le candidat doit également disposer du temps nécessaire pour s'y opposer. La nécessité du contrôle dépend quant à elle, en réalité, des possibilités d'accès et de la confidentialité des données traitées, et non pas forcément du niveau hiérarchique du futur collaborateur[26].

Sous l'angle du droit du travail, l'employeur ne peut traiter que les données qui portent sur l'aptitude[27] du travailleur à remplir son emploi ou celles qui sont nécessaires à l'exécution du contrat. Le contrôle de sécurité s'inscrit dans ce cadre et doit poursuivre ce seul but.

Si elle ne souffre aucune critique sur le plan strict du droit, la solution de l'arrêt du Tribunal fédéral génère néanmoins une situation littéralement inextricable et un résultat choquant : le demandeur d'emploi doit attendre le résultat de la pesée d'intérêt que le tribunal va opérer. Ainsi que le relève Arnold F. Rutsch[28], on ne saurait lui reprocher (ou à son avocat) d'avoir commis une erreur. La banque ne va assurément pas lui faciliter la tâche, de sorte qu'une procédure complexe et onéreuse[29] est à escompter, alors même qu'en définitive il ne s'agit que de l'exercice d'un droit d'accès visant à comprendre pourquoi la banque a refusé de l'engager après avoir émis un avis initial favorable à son sujet. Un tel exercice doit, par

---

contrôle de sécurité dans le secteur public, cf. ATAF A-5013/2019 du 26 août 2020, A. contre Service spécialisé chargé des contrôles de sécurité relatifs aux personnes (Service spécialisé CSP DDPS).

23 Préposé fédéral à la protection des données et à la transparence, Explications relatives aux contrôles de sécurité (employés du secteur privé), mars 2015, accessible à cette adresse : https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/arbeitsbereich/explications-relatives-aux-controles-de-securite--employes-du-se.html

24 Selon le PFPDT, une mention orale suffit dans un premier temps dans le cadre d'un entretien avec un candidat postulant pour un emploi nécessitant un contrôle. Une information écrite devrait intervenir dans un deuxième temps. Cette solution n'est pas optimale, car elle ne permet pas au candidat de vérifier que le contrôle se déroule conformément à la loi. La remise d'une notice informative écrite est susceptible de permettre au candidat d'exercer ses droits en connaissance de cause. La présente affaire démontre à quel point il est difficile d'agir dans un deuxième temps.

25 Spécifiquement lorsque le contrôle intervient par le biais d'une société externe.

26 SYLVAIN MÉTILLE, Les contrôles de sécurité (background check), 11 mars 2015, article publié sur son blog et disponible à cette adresse : https://smetille.ch/2015/05/11/les-controles-de-securite-background-check/ et SYLVAIN MÉTILLE, Internet et droit, Protection de la personnalité et questions pratiques, Quid iuris ?, 20, 2017, pp. 109 et 110.

27 Le mot « aptitude » englobe toutes les données qui sont nécessaires pour déterminer si le travailleur dispose des capacités professionnelles et personnelles objectivement requises pour exercer son activité professionnelle. Il est admis que pour les postes à responsabilité et pour les cadres, certaines qualités personnelles fassent l'objet d'investigations plus poussées. Il en va ainsi de la faculté de coopérer et de diriger, de la confiance en soi, de la résistance au stress, du caractère du salarié, de ses hobbies de sa vision du monde ou de ses ambitions (JEAN-PHILIPPE DUNAND *in* : Jean-Philippe Dunand/Pascal Mahon, Berne 2013, N. 27 *ad* art. 328*b* CO, p. 326).

28 ARNOLD F. RUTSCH, Bundesgericht, I. zivilrechtliche Abteilung, Urteil 4A_83/2020 vom 16. Juli 2020, A. gegen B. AG, vorläufige Einstellung der Vollstreckung, AJP 2020 p. 1634 ss.

29 La seule procédure devant le Tribunal fédéral a généré des coûts de 3'500 francs, n'incluant pas ses frais d'avocat.

essence, demeurer simple et rapide. A défaut, il est inopérant, dans les faits[30]. Même si le candidat obtient *in fine* l'accès à ses données, cela s'apparentera à une victoire à la Pyrrhus, tant il aura dû consacrer du temps, de l'énergie et de l'argent pour atteindre cet objectif.

Rappelons également que ce nœud gordien[31] est le fait de la banque qui a créé une base de données relative à la sécurité des personnes et qui devait donc prévoir l'exercice régulier de droits d'accès et, ainsi, anticiper les problèmes qui auraient pu en résulter[32]. Cette base de données concerne en effet non seulement de potentiels collaborateurs, mais également les collaborateurs qui travaillent pour la banque. Et les tiers intéressés sont également au service de la banque. A l'aune de l'état de fait et des postures procédurales adoptées, une désagréable impression d'entrave peut être ressentie. La banque a, en effet, omis de justifier le souhait de confidentialité des tiers intéressés durant la première procédure, ouvrant la voie à la deuxième et générant les problèmes qui se sont ensuite matérialisés. Et ce dangereux précédent avec le résultat actuel est certainement de nature à la faire persister sur cette voie, pour empêcher l'exercice d'un droit d'accès en cas de litige. Qui serait en effet prêt à investir des milliers de francs en frais de procédure et d'avocat pour un résultat aléatoire ? Plus personne assurément.

De facto, la stratégie de la banque prive également le demandeur d'emploi de toute possibilité d'exercice de ses droits en vertu du droit du travail. Il est également permis de s'interroger sur les suites réservées par une caisse de chômage à une telle situation, paradoxale. Le demandeur d'emploi sera-t-il sanctionné, alors même qu'il ignore pour quel motif, il n'a finalement pas été engagé et que la caisse ne pourra quant à elle en savoir plus ?

Il serait sans doute intéressant, pour le demandeur d'emploi, d'exposer ses difficultés à l'Autorité fédérale de surveillance des marchés financiers[33], laquelle pourrait, dans le cadre de ses attributions en termes de régulation des données, être intéressée à se préoccuper des risques générés par les bases de données relatives à la sécurité des personnes, risques importants (entre autres) en termes de communication des données à l'étranger, de perte, de fuite ou de vols de données. Le fait de laisser se développer de telles bases de données hors

---

30 Pour une analyse éclairante de la discrépance entre les bénéfices théoriques de l'exercice du droit d'accès et la réalité prosaïque, cf. LIVIO DI TRIA/KASTRIOT LUBISHTANI, Etude empirique du droit d'accès à ses données personnelles, *in* : SYLVAIN MÉTILLE (édit.), Le droit d'accès, Berne 2021, p. 52 ss.

31 Il s'agit selon la tradition d'un nœud inextricable qui attachait le joug au timon du char de Gordius, roi de Phrygie, et qu'Alexandre le Grand trancha d'un coup d'épée pour obtenir l'empire d'Asie. Se dit aujourd'hui d'un problème quasi insoluble.

32 Dans un autre contexte, mais avec une analyse similaire s'agissant de la prévisibilité du droit d'accès, cf. CÉLIAN HIRSCH/EMILIE JACOT-GUILLARMOD, Les données bancaires pseudonymisées : du secret bancaire à la protection des données, Revue suisse du droit des affaires et des marchés financiers, 2020, volume 92 n° 2, p. 166 ; la nouvelle loi sur la protection des données imposera cette appréhension initiale des risques dans le cadre notamment de la protection dès la conception (privacy by design), cf. DEBORAH LECHTMAN, L'obligation de « Privacy by Design » en Suisse et son implémentation dans les études d'avocats, Revue de l'avocat 2020 p. 403.

33 Abrégée ci-après FINMA ; https://www.finma.ch/fr/.

du contrôle du PFPDT et des tribunaux[34] est également de nature à susciter des craintes légitimes. Le risque réputationnel, régulièrement évoqué par la FINMA[35], est conséquent.

Les banques suisses, dont certains employés sont au bénéfice de l'une des nationalités de l'Union européenne ou y sont domiciliés[36], seraient bien inspirées de ne pas suivre l'exemple ici commenté. Les régulateurs européens à qui une telle pratique pourrait être annoncée disposent de moyens d'investigation autrement plus incisifs que le PFPDT, et les sanctions qui pourraient être prononcées à leur encontre[37] diffèrent notablement de celles, d'opérette[38], qui figurent dans la nouvelle loi sur la protection des données.

---

[34] Provisoirement et *in parte qua*, la procédure pouvant tout de même aboutir avec des efforts supplémentaires.

[35] Notamment dans la Communication FINMA sur la surveillance 05/2020, cf. SÉBASTIEN FANTI, De l'obligation de signaler les cyberattaques selon l'article 29 al. 2 LFINMA – Communication FINMA sur la surveillance 05/2020, 15 décembre 2020 *in* www.swissprivacy.law/43, accessible à cette adresse : https://swissprivacy.law/43/

[36] Ce qui pourrait fonder une compétence, sans même évoquer les clauses d'application extraterritoriale.

[37] Notamment sur la base du règlement général sur la protection des données, cf. PFPDT, Le RGPD et ses conséquences sur la Suisse, état : mars 2018, accessible à cette adresse : https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2018/Le%20RGPD%20et%20ses%20conséquences%20sur%20la%20Suisse_FR%20Jan%2018.pdf.download.pdf/Le%20RGPD%20et%20ses%20conséquences%20sur%20la%20Suisse_FR%20Jan%2018.pdf.

[38] Pour une comparaison entre les règles du RGPD et de la nLPD : LIVIO DI TRIA, Comparaison entre la nLPD et le RGPD, 12 février 2021 *in* www.swissprivacy.law/55, accessible à cette adresse : https://swissprivacy.law/55/; cf. articles 60 à 65 nLPD, par comparaison avec l'article 83 RGPD.