Intelligence artificielle et automatisation des décisions dans le secteur bancaire et financier : application de la LPD et du RGPD

Hirsch, Célian

How to cite

HIRSCH, Célian. Intelligence artificielle et automatisation des décisions dans le secteur bancaire et financier : application de la LPD et du RGPD. In: Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht, 2024, vol. 96, n° 2, p. 113–126.

This publication URL: https://archive-ouverte.unige.ch/unige:177122

Intelligence artificielle et automatisation des décisions dans le secteur bancaire et financier : application de la LPD et du RGPD

Célian Hirsch*

This article addresses the application of Automated Decision-Making (ADM) in banking and finance, under the revised Swiss Federal Act on Data Protection and the EU's GDPR. It scrutinizes the legal framework of ADM, particularly considering the European Court of Justice's interpretation in the SCHUFA Holding AG case, which broadens the scope of "decision" within the GDPR, encompassing actions like credit scoring. The paper highlights the necessity of meaningful human intervention (human in the loop) in automated processes to avoid classification as ADM. It also contrasts the EU's general prohibition of ADM, subject to exceptions, with Switzerland's emphasis on informational rights. The discussion extends to the consequences of violating ADM regulations, comparing EU and Swiss approaches. Concluding, the implementation of ADM regulation in Switzerland is seen as being influenced by individual rights exercise, regulatory oversight, and responsiveness to rights infringements.

Table des matières

I. Introduction

En mai 2021, l'Association suisse des banquiers (ASB) dévoile son Guide sur la « Gestion des données dans les activités bancaires courantes »[1]. Alors que le grand public n'a pas encore découvert les exploits de l'intelligence artificielle – nous sommes avant l'ère de ChatGPT –, l'ASB examine déjà six cas d'utilisation de l'intelligence artificielle, tels que la compliance, l'examen de crédit *(credit scoring)* ou encore l'authentification biométrique. Consciente de la problématique essentielle de la protection des données, et plus particulièrement des décisions individuelles automatisées (DIA), l'ASB souligne que :

> « S'il devait arriver que les décisions soient prises exclusivement par des systèmes d'IA, sans intervention d'un collaborateur de la banque, il y aura lieu d'examiner leurs éventuelles conséquences juridiques au regard des dispositions sur les décisions individuelles automatisées (art. 21 [LPD]) et, le cas échéant, d'en tenir compte. »[2]

Les banques ne sont évidemment pas les seules à profiter des développements de l'intelligence artificielle. Les *Fintech* et autres entreprises technologiques ont particulièrement augmenté l'offre de services automatisés. Lors de l'entrée en relation client, le prestataire de services bancaires et financiers peut procéder à un *onboarding* automatisé[3] ainsi qu'à un *screening* automatique des listes des PEP et des personnes sous sanctions. Au début de la relation, le prestataire peut également compter sur un processus sans interaction humaine afin d'établir le profil client, voire la stratégie d'investissement. Ensuite, l'achat et la vente de produits financiers peuvent également être automatisés, comme le proposent les sociétés de gestion de fortune automatisée *(robo advisor)*. Par ailleurs, si le client dé-

* Dr *Célian Hirsch*, avocat, est maître-assistant au Centre de droit bancaire et financier de l'Université de Genève. Il est également lecteur à l'Université de Fribourg. Me *Nathan Matantu* est remercié infiniment en raison de sa précieuse relecture et de ses commentaires pertinents.

1 Association suisse des banquiers, Gestion des données dans les activités bancaires courantes, mai 2021. Sur la notion de données bancaires, cf. *Hirsch Célian*, Le devoir d'informer lors d'une violation de la sécurité des données, Avec un regard particulier sur les données bancaires, thèse, Genève 2023, p. 51 ss.

2 Association suisse des banquiers (n. 1), p. 14.

3 Cf. la Circulaire 2016/7 de la FINMA sur l'identification par vidéo et en ligne du 3 mars 2016.

sire obtenir un crédit, un examen de sa solvabilité peut aussi être effectué sans intervention humaine. Enfin, un algorithme peut analyser toutes les transactions afin de repérer celles qui présentent un risque de fraude ou de blanchiment d'argent afin de les bloquer temporairement, voire de bloquer le compte, jusqu'à une vérification humaine subséquente.

Ces divers services automatisés correspondent-ils à des DIA ? Le cas échéant, avec quelles conséquences pour le prestataire ? Et que risque le prestataire qui ne respecterait pas les conséquences juridiques découlant de l'existence d'une DIA ?

Afin de répondre à ces questions, la présente contribution expose les DIA dans le secteur bancaire et financier, à l'aune tant du droit de l'Union européenne (UE) que du droit suisse (LPD).

Même pour les prestataires sis en Suisse, l'analyse du droit de l'UE est pertinente à double titre. En premier lieu, le Règlement général sur la protection des données (RGPD) prévoit un important effet extraterritorial : il s'applique aux responsables du traitement sis en Suisse lorsqu'ils offrent des biens ou des services à des personnes domiciliées dans l'UE ou lorsqu'ils suivent le comportement de ces personnes (art. 3 par. 2 RGPD)[4]. En second lieu, le droit suisse de la DIA est grandement inspiré de celui adopté par l'UE[5] ; le droit de l'UE est donc pertinent pour interpréter le droit suisse[6].

Après avoir défini la notion de décision individuelle automatisée (DIA) (II), la contribution examine les conséquences juridiques d'une DIA (III) ainsi que les exceptions (IV). Elle expose ensuite les conséquences en cas de violation des obligations légales (V) et développe certaines perspectives (VI) avant de conclure (VII).

II. Définition de la décision individuelle automatisée (DIA)

La notion de décision individuelle automatisée (DIA) provient de l'art. 22 par. 1 RGPD. Selon cette disposition, il s'agit « d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques (…) concernant [la personne visée par la décision] ou l'affectant de manière significative de façon similaire ». Le législateur suisse a repris cette notion à l'art. 21 LPD et définit la DIA comme « toute décision qui est prise exclusivement sur la base d'un traitement de données personnelles automatisé et qui a des effets juridiques pour [la personne concernée] ou l'affecte de manière significative ».

L'existence d'une DIA est donc soumise aux trois conditions cumulatives suivantes :

1. Une décision ;
2. Exclusivement automatisée ;
3. Qui déploie des effets juridiques pour la personne concernée ou l'affecte de manière significative.

1. Une décision …

Ni le RGPD ni la LPD ne définissent ce qu'il faut comprendre par « décision » *(decision ; Entscheidung)*. Alors qu'une notion (trop) large semble se profiler au sein de l'UE, la Suisse pourrait (et devrait) aller dans le sens opposé[7].

1.1 La notion large au sens du RGPD

Selon la doctrine allemande, l'exigence d'une décision requiert que le résultat du traitement automatisé des données soit un acte imputable à une personne phy-

4 Comité européen de la protection des données, Lignes directrices 3/2018 sur l'application territoriale du RGPD (art. 3), 12 novembre 2019 ; Préposé fédéral à la protection des données et à la transparence, Le RGPD de l'UE et ses conséquences sur la Suisse, juillet 2018 ; *Métille Sylvain/Ackermann Annelise,* RGPD : application territoriale et extraterritoriale, in : Epiney Astrid/Rovelli Sophia (édit.), Datenschutzgrundverordnung (DSGVO) : Tragweite und erste Erfahrungen / Le Règlement général sur la protection des données (RPDG) : portée et premières expériences, Genève/Zurich/Bâle 2020, p. 81 ss ; *Benhamou Yaniv/Jacot-Guillarmod Emilie,* RGPD sur sol suisse : mise en œuvre, digma 2018, p. 142 ss.

5 Concernant l'influence du RGPD dans la révision totale de la LPD, cf. *Hirsch* (n. 1), p. 126 ss.

6 Sur l'influence du RGPD dans l'interprétation de la LPD, cf. *Hirsch* (n. 1), p. 130 ss.

7 La notion de DIA est la même selon le RGPD et selon le droit suisse (*Hirsch Célian/Merlino Nastasia,* Do Robots Rule Wealth Management ? A Brief Legal Analysis of Robo-Advisors, RSDA 2022, p. 44 ; cf. ég. *Henseler Simon/Vasella David,* Art. 21 DSG, in : Blechta Gabor/Vasella David (édit.), Datenschutzgesetz/Öffentlichkeitsgesetz, Basler Kommentar, Bâle 2024, Art. 21 N 8). Cela étant, l'interprétation effectuée par la CJUE de la notion de DIA ne lie pas directement les tribunaux suisses (sur l'influence du RGPD dans l'interprétation de la LPD, cf. *Hirsch* [n. 1], p. 130 ss).

sique ou morale, qui choisit entre au moins deux variantes et qui a, dans une certaine mesure, un effet définitif[8].

Dans l'arrêt C-634/21 du 7 décembre 2023 (SCHUFA Holding AG), la Cour de justice de l'Union européenne (CJUE) a considéré que le *credit scoring* effectué par l'entreprise allemande SCHUFA constitue une DIA[9].

Concrètement, SCHUFA « établit un pronostic sur la probabilité d'un comportement futur d'une personne *(‹ score ›)*, tel que le remboursement d'un prêt, à partir de certaines caractéristiques de cette personne, sur la base de procédures mathématiques et statistiques. L'établissement des scores *(‹ scoring ›)* est fondé sur l'hypothèse selon laquelle il est possible, en assignant une personne à un groupe d'autres personnes possédant des caractéristiques comparables et qui se sont comportées d'une manière donnée, de prédire un comportement similaire »[10].

Dans la procédure, SCHUFA soutient qu'elle ne prend pas de décision d'octroi de crédit, mais communique simplement ce score à un partenaire contractuel. Ce dernier se fonde alors « de manière déterminante » sur le score de solvabilité communiqué afin de décider de l'octroi d'un crédit. Dans cet arrêt, la CJUE se penche ainsi sur la notion de « décision » (première condition de la DIA)[11].

Le considérant 71 du RGPD cite comme exemples de DIA « le rejet automatique d'une demande de crédit en ligne ». La Cour en déduit que la notion de « décision » revêt une portée « suffisamment large pour englober le résultat du calcul de la solvabilité d'une personne sous la forme d'une valeur de probabilité concernant la capacité de cette personne à honorer des engagements de paiement à l'avenir ».[12]

Partant, selon la CJUE, le simple fait d'effectuer un *credit scoring* constitue déjà une décision au sens de l'art. 22 RGPD, même si le responsable du traitement ne fait ensuite que transmettre ce score de solvabilité à un tiers, sans prendre lui-même la décision d'octroi de crédit.

Cette jurisprudence semble élargir considérablement la portée de la notion de décision[13]. Toute société qui décide d'évaluer de manière automatisée des personnes concernées selon certaines caractéristiques prendrait une décision dès lors qu'un tiers se fonderait sur cette évaluation afin de décider de l'octroi d'un service. Ainsi, le prestataire, qui utilise un algorithme afin d'évaluer si certaines transactions sont frauduleuses, prendrait déjà une décision au sens de l'art. 22 RGPD, même si c'est ensuite la banque qui décide de bloquer la transaction.

8 *Schulz Sebastian,* in : Gola Peter/Heckmann Dirk (édit.), Datenschutz-Grundverordnung, 3e éd., Munich 2022, Art. 22 N 17. Cf. ég. BSK DSG-*Henseler/Vasella* (n. 7), Art. 21 N 10. Cf. ég. *Bygrave* qui considère que la décision doit avoir *« a degree of binding effect »* (*Bygrave Lee A.*, Article 22 GDPR, Automated individual decision-making, including profiling, in : Kuner Christopher/Byygrave Lee A./Docksey Christopher/Drechsler Laura [édit.], The EU General Data Protection Regulation (GDPR) : A Commentary, Oxford University Press 2020, p. 532).
Afin de limiter la portée de la « décision », la doctrine allemande considère qu'une décision générale et abstraite ne constitue pas une DIA, contrairement aux décisions individuelles et concrètes, en référence aux décisions de droit administratif (*von Lewinski Kai,* Art. 22 DS-GVO Automatisierte Entscheidungen im Einzelfall einschliesslich Profiling, in : Wolff Heinrich A./Brink Stefan/v. Ungern-Sternberg Antje [édit.], BeckOK Datenschutzrecht, 46e éd., Munich 2023, Art. 22 N 15). Pour le droit suisse, cf. *Henseler Simon,* Was ist eine automatisierte Entscheidung ? Zum Tatbestand von Art. 22 Abs. 1 DSGVO, in: Meier Julia/Zurkinden Nadine/Staffler Lukas (édit.), Recht und Innovation, Innovation durch Recht, im Recht und als Herausforderung für das Recht, Zurich 2020, p. 301 ss. La Prof. *Brkan* soutient de façon convaincante qu'une décision concernant un groupe doit être considérée comme un ensemble de décisions individuelles et n'échappe donc pas à la notion de décision (*Brkan Maja,* Do Algorithms Rule the World ? Algorithmic Decision-Making in the Framework of the GDPR and Beyond, International Journal of Law and Information Technology, Summer 2019, 27/2, p. 9. Cf. ég. dans le même sens BSK DSG-*Henseler/Vasella* [n. 7], Art. 21 N 13).

9 CJUE, C-634/21, OQ contre Land Hessen, en présence de SCHUFA Holding AG, 7 décembre 2023, ECLI : EU : C : 2023 : 957, commenté in : *Hirsch Célian,* Décision individuelle automatisée : La société de *credit scoring* doit informer les personnes concernées, publié le 4 janvier 2024 par le Centre de droit bancaire et financier, *<https://cdbf.ch/1316/>*.

10 *Id.,* par. 14.

11 *Id.,* par. 45

12 *Id.,* par. 46.

13 Pour une critique de cette jurisprudence, cf. *Hirsch* (n. 9) ; *Henseler Simon,* EuGH C-634/21 : Kreditscore (der SCHUFA) als automatisierte Entscheidung, 8 décembre 2023 *(<https://datenrecht.ch/eugh-c-634-21-kreditscore-der-schufa-als-automatisierte-entscheidung/>)* ; *Paal Boris,* Case Note : Article 22 GDPR : Credit Scoring Before the CJEU, Global Privacy Law Review, 2023/3, vol. 4, p. 127 ss ; *Paal Boris,* Art. 22 DS-GVO Kreditscoring vor dem EuGH, Zeitschrift für Digitalisierung und Recht 2023, p. 114 ss. Plus convaincu par cet arrêt, cf. *Montavon Michael,* La CJUE serre la vis au traitement des données par les sociétés de fourniture de renseignements commerciaux , 18 décembre 2023, in : *<www.swissprivacy.law/274>*.

Dans son arrêt, la CJUE part de la prémisse que le partenaire contractuel de SCHUFA, qui prend la décision d'octroi de crédit, ne disposerait pas des informations qu'il devra divulguer à la personne concernée conformément au RGPD. De ce fait, la CJUE justifie sa solution par le fait qu'il « existerait un risque de contournement de l'article 22 du RGPD et, par suite, une lacune dans la protection juridique si une interprétation restrictive de cette disposition était retenue, selon laquelle l'établissement de la valeur de probabilité doit seulement être considéré comme un acte préparatoire et seul l'acte adopté par [le partenaire contractuel] peut, le cas échéant, être qualifié de ‹ décision › »[14].

Or, cette prémisse nous semble inexacte. En effet, le partenaire contractuel est considéré comme un responsable du traitement soumis au RGPD et au devoir d'informer[15]. Il ne peut prendre de DIA sans assumer les obligations qui en découlent[16]. En particulier, il doit informer la personne concernée de la DIA et de la logique sous-jacente[17]. En pratique, le partenaire contractuel d'une société qui effectue des évaluations devrait s'assurer que le contrat lui permette d'obtenir de cette société les informations nécessaires sur les évaluations reçues. Ainsi, la banque qui octroie des crédits de manière automatisée devrait prévoir contractuellement qu'elle obtiendra les informations utiles sur la méthode et les données d'évaluation utilisées par la société de *credit scoring.*

En résumé, au vu de l'appréciation de la Cour, tout prestataire qui procède à des évaluations automatisées de clients afin qu'un tiers se fonde sur cette évaluation pour décider de l'octroi d'une prestation doit examiner attentivement s'il tombe sous le coup de cette jurisprudence. Cela vaut en particulier pour les *Regtech,* car ces sociétés visent précisément à automatiser, grâce à l'intelligence artificielle, un ou plusieurs processus tels que le KYC pour le *onboarding* ou le *screening* des listes des PEP et des personnes sous sanctions. La banque se fonde ensuite de manière déterminante sur ce processus pour prendre une décision.

14 *Id.,* par. 61.

15 Cf. art. 15 par. 1 let. e RGPD et art. 25 al. 2 let. f LPD.

16 Cf. *infra* III.1.

17 Concernant le devoir d'informer de la logique sous-jacente, cf. *infra* III.

1.2 Une notion restreinte en droit suisse

En droit suisse, le Message du Conseil fédéral limite la notion de décision à celles présentant « un certain degré de complexité »[18]. Ainsi, « [l]es décisions simples [décisions ‹ si-alors ›] du genre de celles qui sont prises lors d'un retrait au bancomat (délivrance du montant demandé si le solde en compte est suffisant) » ne constituent pas des ‹ décisions › »[19]. Dit autrement, le responsable du traitement doit avoir un certain pouvoir d'appréciation *(Ermessenentscheid)*[20] afin de pouvoir prendre une décision discrétionnaire[21]. Les décisions prises par une intelligence artificielle répondront très généralement à cette exigence.

Par ailleurs, la jurisprudence SCHUFA pourrait ne pas être reprise en droit suisse. En effet, comme le souligne Henseler[22], le Conseil fédéral considère que « [l]e calcul d'un score de solvabilité par une société de renseignement ne constitue pas une décision individuelle automatisée au sens de la [LPD] mais une aide à la décision dans la mesure où la décision effective (refus d'un paiement sur facture, par ex.) appartient au client de la société »[23].

18 Conseil fédéral, Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017, FF 2017, p. 6674. Pour une analyse de la notion de « décision » au sens de la DIA en droit suisse, cf. *Suter Fabienne,* Automatisierte Einzelentscheidungen im (Schweizer) Datenschutzrecht Phänomen, Entstehungsgeschichte, Regelungsziele und Begriff, thèse, Zurich 2024 (à paraître), X.3.2. Cette auteure critique en particulier cette exigence de complexité.

19 *Id.* Le Message en allemand mentionne expressément les « *reine Wenn-Dann Entscheidungen* » alors que le texte français ne parle que de « décisions simples ». Sur l'exigence de complexité, cf. BSK DSG-*Henseler/Vasella* (n. 7), Art. 21 N 16 qui soutiennent que la complexité concerne l'objet de la décision et non pas le processus décisionnel.

20 *Rosenthal David,* Das neue Datenschutzgesetz, Jusletter 16 novembre 2020, N 107.

21 *Mehmedovic Senida,* Le droit d'accès à une décision individuelle automatisée, Jusletter 19 septembre 2022, N 28 ; *Flueckiger Christian,* in : Métille Sylvain/Meier Philippe (édit), Commentaire Romand, Loi sur la protection des données, Bâle 2023, Art. 22 N 2.

22 *Henseler* (n. 13).

23 Conseil fédéral, Encadrement des pratiques des sociétés de renseignement de solvabilité, Rapport du Conseil fédéral donnant suite au postulat 16.3682 Schwaab du 21 septembre 2016, p. 25. Cf. ég. *Wermelinger Amédéo,* Bonitätsbeurteilung und datenschutzrechtlich hohes Risiko, Jusletter 22 janvier 2024, N 49, pour une analyse des effets de cet arrêt en Suisse.

L'approche du Conseil fédéral nous semble convaincante et devrait être reprise par nos tribunaux. En effet, le législateur suisse, même s'il s'est inspiré du RGPD, vise les décisions rendues, et non les simples évaluations telle que l'attribution d'un score de solvabilité. Or, la décision d'octroyer le crédit est effectivement prise par le prestataire lui-même. Pour sa part, la société de *credit scoring* ne prend pas de décision, mais effectue une simple évaluation. Elle n'est d'ailleurs pas en relation directe avec le demandeur de crédit. Retenir l'inverse élargirait le champ d'application de la DIA, sans pour autant qu'une telle solution soit justifiée par l'une des quatre méthodes d'interprétation[24].

Partant, les *Fintech* suisses qui ne procèdent qu'à des évaluations, sans être soumises au RGPD[25], ne prennent pas de décision au sens de la DIA. Seul le prestataire qui utilise ces évaluations prend une décision. Il convient encore de vérifier si celle-ci est « exclusivement automatisée » afin qu'elle puisse être qualifiée de DIA.

2. … exclusivement automatisée …

La DIA suppose que la décision soit « prise exclusivement sur la base d'un traitement de données personnelles automatisé » *(based solely on automated processing* ; *die ausschliesslich auf einer automatisierten Bearbeitung beruht[26]).* Toute intervention humaine suffit-elle à exclure une DIA ? La réponse est négative. En effet, « [p]our qu'il y ait intervention humaine, le responsable du traitement doit s'assurer que tout contrôle de la décision est significatif et ne constitue pas qu'un simple geste symbolique »[27]. Cette problématique est particulièrement présente lorsqu'un algorithme propose une décision (proposition automatisée) qui est ensuite revue par un humain[28].

La doctrine retient qu'en cas de proposition automatisée, l'intervention humaine *(human in the loop)* exclut l'existence d'une DIA si cinq conditions cumulatives sont réunies :

1. L'humain peut s'écarter de la proposition automatisée ; en d'autres termes, il dispose d'une marge d'appréciation ;
2. Il dispose de la compétence appropriée pour prendre la décision ;
3. Il dispose des qualifications et aptitudes professionnelles pour pouvoir vérifier la proposition automatisée ;
4. Il est suffisamment instruit et connaît les données nécessaires à la prise de proposition automatisée ; et
5. Il intervient avant la prise de décision, mais après la proposition automatisée[29].

Lorsque ces cinq conditions sont remplies, la proposition automatisée revue par un humain ne constitue pas une décision exclusivement automatisée. Par conséquent, il n'y a pas de DIA.

En pratique, démontrer le respect des cinq conditions susmentionnées peut s'avérer délicat. Une possibilité pour le responsable du traitement consiste à documenter les décisions (humaines) qui s'écartent des propositions automatisées. S'il en existe suffisamment, cela peut démontrer qu'il existe une réelle intervention humaine, et donc l'absence de DIA[30].

Cela étant, l'intelligence artificielle avec une capacité d'autoapprentissage peut assimiler les circonstances dans lesquelles l'humain s'écarte de ses recommandations. Par conséquent, elle améliorera ses propositions automatisées, ce qui réduira les situations dans lesquelles l'humain intervient, avec le risque que l'intervention ne soit plus suffisante afin d'exclure l'existence d'une DIA.

En pratique, le prestataire de services bancaires et financiers doit déterminer, pour chaque service automatisé s'il peut et veut respecter les conditions de *human in the loop* afin d'exclure l'existence de DIA. Le cas échéant, il doit choisir et former une personne compétente pour chaque service automatisé. Celle-ci devra

24 Concernant les diverses méthodes d'interprétation, cf. CR CC I-*Werro,* 2e éd. 2023, art. 1 N 65 ss ; BSK ZGB I-*Honsell,* 7e éd. 2022, art. 1 N 9 ss.

25 Cf. n 4.

26 Les textes français et allemand du RGPD diffèrent très légèrement du texte suisse : « fondée exclusivement sur un traitement automatisé » ; *« ausschliesslich auf einer automatisierten Verarbeitung beruhenden Entscheidung ».*

27 Groupe de travail « Article 29 » sur la protection des données (G29), Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, adoptées le 3 octobre 2017 et révisées le 6 février 2018, p. 23.

28 Pour une analyse précise de cette problématique, cf. *Binns Reuben/Veale Michael,* Is That Your Final Decision? Multi-Stage Profiling, Selective Effects, and Article 22 of the GDPR, International Data Privacy Law, November 2021, 11/4, p. 319–332.

29 *Hensler* (n. 8), p. 306 ss ; *von Lewinski* (n. 8), Art. 22 DGSVO N 24 ss.

30 *Hirsch/Merlino* (n. 7), p. 41 s.

effectivement revoir les décisions proposées par l'algorithme afin d'exclure l'existence d'une DIA.

En revanche, si le prestataire vise un processus exclusivement automatisé, comme le *robo advisor* ou le *screening* de transactions potentiellement frauduleuses, il convient encore d'examiner si ses décisions produisent des effets significatifs[31].

3. … avec des effets significatifs

Enfin, la décision doit soit avoir des effets juridiques pour la personne concernée, soit l'affecter de manière significative *(produces legal effects concerning him or her or significantly affects him or her ; die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt)*[32].

Tant les effets juridiques que l'atteinte significative doivent avoir « une incidence grave » pour la personne concernée[33]. En effet, les législateurs européen et suisse ne pouvaient pas avoir pour intention de considérer comme des DIA toutes les décisions automatisées produisant des effets juridiques, y compris celles n'affectant (presque) pas la personne concernée[34]. Cela irait d'ailleurs au-delà du but visé par les obligations découlant de la DIA (interprétation téléologique restrictive).

Retenir l'inverse reviendrait à considérer chaque transaction effectuée par un *robo advisor* comme une DIA. En effet, celui-ci achète et vend des instruments financiers pour le compte du client. Chaque transaction décidée par l'algorithme produit donc des effets juridiques pour le client, puisqu'il devient détenteur d'un produit financier ou perd cette détention. Or, il n'est pas justifié de considérer chaque transaction comme une DIA. Même l'ensemble des transactions effectuées par le *robo advisor* ne doit pas être considéré comme une DIA s'il ne peut pas en découler d'incidence grave pour le client, par exemple parce que seule une infime partie de son patrimoine total est géré par ce *robo advisor*[35].

Il en va de même pour la décision automatisée qui suspend l'exécution d'une transaction en raison d'une suspicion de fraude ou de violation des règles contre le blanchiment d'argent. Une telle décision automatisée, qui déploie des effets juridiques en raison de la suspension d'une transaction, ne déploie pas forcément des effets d'une certaine gravité pour le client. Elle doit par conséquent être considérée comme une DIA uniquement lorsqu'elle peut effectivement avoir « une incidence grave » pour le client[36], en particulier selon l'importance (absolue ou relative) du montant de la transaction.

Partant, lors de chaque décision automatisée – par exemple l'octroi d'un crédit, le *screening* d'une transaction potentiellement frauduleuse, ou encore l'achat ou la vente automatisée d'instruments financiers *(robo advisor)* –, il convient d'examiner objectivement les conséquences pour le client, en tenant notamment compte de sa situation financière. Seules les décisions d'une certaine gravité doivent être considérées comme des DIA. En pratique, il peut être plus simple pour le prestataire qui prend des DIA de considérer toutes ses décisions automatisées comme des DIA. Cela lui éviterait de devoir examiner si chaque décision automatisée déploie des effets significatifs. Par conséquent, il devrait dans tous les cas respecter les conséquences juridiques décrites ci-dessous.

III. Régime juridique de la DIA

1. Les conséquences selon l'art. 22 RGPD

L'art. 22 par. 1 RGPD prévoit une interdiction générale des DIA[37]. Cette interdiction est fondée sur le principe

31 *Infra* II.3.

32 Le texte du RGPD diffère ici très légèrement du texte suisse. Le premier indique que la décision doit affecter la personne concernée « de façon similaire » *(similarly ; in ähnlicher Weise)* à une décision qui produit des effets juridiques. Malgré cette différence de texte, la notion suisse de DIA correspond à celle du RGPD (BSK DSG-*Henseler/Vasella* [n. 7], Art. 21 N 8).

33 G29 (n. 27), p. 23. Cf. ég. le rapport explicatif relatif à l'AP-LPD qui parle d'effets « d'une certaine gravité » (Office fédéral de la justice, Rapport explicatif concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales, 21 décembre 2016, p. 57). Cf. ég. *Suter* (n. 18), X.3.2.d).i.

34 Cette justification repose sur une interprétation téléologique (*contra* BSK DSG-*Henseler/Vasella* [n. 7], Art. 21 N 29).

35 *Hirsch/Merlino* (n. 7), p. 43.

36 *Contra Hensler* (n. 8), 311.

37 Ce principe remonte à l'art. 2 de la Loi française n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (cf. *Suter* [n. 18], VII). La doctrine européenne a débattu de longues années afin de déterminer si l'art. 22 RGPD impose une interdiction de principe ou prévoit uniquement un droit en faveur des personnes concernées (cf. not. *Tosoni Luca*, The Right to Object to Automated Individual Decisions : Resolving the Ambiguity of Article 22(1) of the General Data Protection Regulation, International

que les décisions affectant la vie des humains ne devraient pas être laissées à la discrétion des machines[38]. Cependant, comme tout principe juridique, celui-ci admet des exceptions qui seront examinées plus bas[39]. Lorsqu'une DIA est prise dans le cadre de ces exceptions, le RGPD impose des obligations spécifiques de transparence et de responsabilité.

Premièrement, la personne concernée par une telle décision doit être informée spontanément non seulement de l'existence de la décision automatisée, mais aussi de la « logique sous-jacente » *(the logic involved ; die involvierte Logik)* sur laquelle elle repose[40]. Le responsable du traitement doit « trouver des moyens simples d'informer la personne concernée de la raison d'être de la décision ou des critères sur lesquels elle est fondée »[41]. Cela étant, ce droit d'être informé n'est pas absolu. En effet, le considérant 63 du RGPD mentionne deux limites : le secret des affaires et la propriété intellectuelle[42].

Dans un arrêt du 29 juin 2023, le *Bundesverwaltungsgericht* autrichien s'est penché sur la demande d'une personne concernée qui voulait accéder à plus d'informations concernant son score de solvabilité. Le tribunal a considéré que la communication des différentes variables était suffisante, le responsable du traitement ne devant pas indiquer la pondération de chaque variable. En effet, cela reviendrait à divulguer l'algorithme, lequel n'est pas compris par le droit d'accès[43]. Cela étant, avec les seules variables, mais sans la pondération, nous doutons que la personne concernée puisse réellement comprendre « les raisons de la décision »[44].

Dans une décision du 28 mars 2022, l'autorité suédoise de protection des données a sanctionné une banque en raison du manque d'informations relatives à la logique sous-jacente dans sa *privacy policy.* La banque indiquait bien l'utilisation de DIA pour l'octroi de crédits, mais n'indiquait ni l'utilisation de son propre modèle de *credit scoring,* ni les catégories de données utilisées à cette fin[45]. Le prestataire doit en effet respecter son obligation de transparence quant à la logique sous-jacente déjà dans sa politique de protection des données[46], et non uniquement lorsqu'il communique la décision à la personne concernée (au contraire du droit suisse qui impose d'informer de la logique sous-jacente uniquement sur demande de la personne concernée, cf. *infra* 2).

Une information plus précise peut également être communiquée avec la décision. Le prestataire peut en particulier donner une explication hypothétique afin de justifier celle-ci, par exemple : si vous aviez eu un salaire de X% plus élevé, vous auriez reçu le crédit demandé, respectivement vous auriez reçu un crédit

Data Privacy Law, April 2021, 11/2, p. 145–162). La CJUE a récemment tranché (très brièvement) cette controverse : « Cette disposition édicte une interdiction de principe dont la méconnaissance ne nécessite pas d'être invoquée de manière individuelle par une telle personne. » (CJUE, C-634/21, OQ contre Land Hessen, en présence de SCHUFA Holding AG, 7 décembre 2023, ECLI :EU :C :2023 :957, par. 52).

38 *Bensamoun Alexandra/Loiseau Grégoire,* Droit de l'Intelligence Artificielle (2019), p. 281 ; *Martini Mario,* Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz, Berlin, 2019, p. 170. Pour une brève analyse d'un point de vue éthique, cf. *Thouvenin Florent/Früh Alfred/George Damian,* Datenschutz und automatisierte Entscheidungen, Jusletter 26 novembre 2018, N 16 ss.

39 Cf. *infra* IV.1.

40 Art. 13 par. 2 let. f RGPD ; art. 14 par. 2 let. g RGPD et art. 15 par. 1 let. h RGPD.

41 G29 (n. 27), p. 28. Cf. en particulier *Wachter Sandra/Mittelstadt Brent/Russel Chris,* Counterfactual Explanations Without Opening the Black Box : Automated Decisions and the GDPR, Harvard Journal of Law & Technology, Spring 2018, 31/2, p. 878. Cf. ég. *Hirsch/Merlino* (n. 7), p. 47 ss.

42 Sur la tension entre, d'une part, l'information relative à la DIA et, d'autre part, le secret des affaires et la propriété intellectuelle, cf. *Gözde Aracı*, A Quest for Fair Balance : Testing the Right of Access against IP Rights and Trade Secrets, September 2019, MIPLC Master Thesis Series (2018/19).

43 Arrêt du *Bundesverwaltungsgericht* autrichien, W252 2246581-1/6E, du 29 juin 2023, p. 7. Le G29 considère également que « [l]e RGPD exige que le responsable du traitement fournisse des informations utiles sur la logique sous-jacente, mais pas nécessairement une explication complexe des algorithmes utilisés ou la divulgation de l'algorithme complet » (G29 [n. 27], p. 28). Cf. ég. *Winkler Markus,* Credit Scoring, AML Software & Risk Profiling : Automatisierte Entscheidungen im Rahmen von Finanzdienstleistungen, RSDA 2020, p. 71 ; *Rosenthal* (n. 20), p. 46 N 119 ; *Stengel Cornelia/Wirthensohn Gino/Stäuble Luca,* Regulierung von künstlicher Intelligenz für FinTech-Anwendungen, RSDA 2021, p. 407.

44 G29 (n. 27), p. 28.

45 *Integritetsskyddsmyndigheten,* DI-2019-4062, 28 mars 2022, p. 39 s. (pour un résumé en anglais cf. <*https://gdprhub.eu/index.php?title=IMY_(Sweden)_-_DI-2019-4062*>).

46 Le devoir d'informer de la logique sous-jacente trouve en effet sa source dans les obligations générales de transparences, lesquelles doivent être respectées au plus tard un mois après l'obtention des données personnelles (art. 14 par. 3 let. a RGPD).

avec un meilleur taux d'intérêt[47]. De cette manière, sans dévoiler la pondération et l'algorithme, le responsable du traitement peut dévoiler à la personne concernée de quelle façon elle aurait pu bénéficier d'une meilleure décision, respectant ainsi son devoir d'informer.

La question de l'information qui doit être communiquée à la personne concernée, y compris l'algorithme et sa relation avec le secret d'affaires, fait précisément l'objet d'une procédure pendante devant la CJUE[48]. Espérons que cette future décision permettra de clarifier cette délicate situation.

Deuxièmement, les personnes concernées doivent être informées de « l'importance et les conséquences prévues de ce traitement » *(the significance and the envisaged consequences of such processing ; die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung)*[49]. Par exemple, un prestataire qui recourt à un *onboarding* automatisé devra expliquer au potentiel client que la DIA aura pour conséquence qu'il sera admis, ou non, comme client. Le prestataire qui utilise un *robo advisor* (qui a des effets significatifs[50]) devra communiquer au client les effets que ces décisions automatisées peuvent avoir sur l'évolution de son patrimoine investi[51].

Troisièmement, la personne concernée a le droit de demander une intervention humaine, d'exprimer son point de vue et de contester la DIA. Le prestataire de services bancaires et financiers automatisés doit mettre en place un processus qui permette à la personne concernée par la DIA d'exercer valablement ce droit d'être entendu. Il doit prévoir qu'un humain compétent puisse « procéder à une évaluation approfondie de toutes les données pertinentes, y compris toute information supplémentaire fournie par la personne concernée »[52]. Cela permet par exemple à la personne qui s'est vu refuser l'entrée en relation avec une banque, respectivement refuser un crédit, de contester ce refus et d'expliquer pourquoi elle devrait pouvoir bénéficier du service requis.

Enfin, le responsable du traitement qui envisage de mettre en œuvre des DIA doit effectuer une analyse d'impact relative à la protection des données (AIPD)[53]. Cette analyse évalue les conséquences potentielles pour les personnes concernées et identifie les mesures susceptibles de minimiser les impacts négatifs des DIA[54]. Elle ne doit cependant pas être rendue publique ou mise à disposition des personnes concernées[55], mais peut devoir être communiquée à l'autorité de protection des données compétente[56]. Le prestataire doit procéder à cette analyse préalablement à la mise en œuvre des DIA. Il peut ainsi prouver qu'il est conscient des risques liés aux DIA et qu'il a identifié et pris les mesures qui réduisent dans la mesure du possible les conséquences négatives découlant du processus automatisé. A notre avis, il peut par exemple déterminer dans l'AIPD les moyens de communication de l'information idoine et son contenu, selon que celle-ci soit transmise à la personne concernée préalablement – typiquement dans une *privacy policy* – ou au moment de la DIA. L'AIPD devrait aussi identifier les interventions humaines qui permettent de réduire les potentielles conséquences négatives découlant du processus automatisé, par exemple à l'aide d'une vérification par un employé d'un échantillon de décisions.

47 *Wachter/Mittelstadt/Russel* (n. 41), p. 844.

48 Demande de décision préjudicielle présentée par le *Verwaltungsgericht* de Vienne le 16 mars 2022 – CK, Affaire C-203/22.

49 Art. 13 par. 2 let. f RGPD ; art. 14 par. 2 let. g RGPD et art. 15 par. 1 let. h RGPD.

50 Cf. *supra* II.3.

51 Le prestataire doit en plus respecter son devoir d'informer découlant de la LSFin (art. 8 al. 1 et al. 2 LSFin) et celui découlant du mandat (art. 398 al. 2 CO) (*Hirsch/Merlino* [n. 7], p. 38 s.).

52 G29 (n. 27), p. 28. *von Lewinski* (n. 8), Art. 22 DGSVO N 48 ss ; *Martini Mario,* Art. 22 Automatisierte Entscheidungen im Einzelfall einschliesslich Profiling, in : Paal Boris P./ Pauly Daniel A. (édit.), Beck'sche Kompakt-Kommentare, Bundesdatenschutzgesetz, 3e éd., Munich 2021, Art. 22 N 39c.

53 Art. 35 RGPD ; G29 (n. 27), p. 33.

54 Art. 35 par. 7 RGPD. Pour un exemple d'une telle analyse d'impact, cf. le Data Protection Impact Asessment du 1er mai 2020 effectué par *id est avocats* concernant le modèle Decentralized Privacy-Preserving Proximity Tracing *(<https://github.com/DP-3T/documents/blob/master/data_protection/DP-3T%20Model%20DPIA.pdf>).* Cf. ég. *di Tria Livio,* L'analyse d'impact relative à la protection des données (AIPD) en droit européen et suisse, sic ! 2020, p. 119 ss.

55 *Martini* (n. 38), p. 210.

56 Groupe de travail « Article 29 » sur la protection des données, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, adoptées le 4 octobre 2017, p. 21.

2. Les conséquences selon l'art. 21 LPD

Contrairement à l'UE, où l'art. 22 RGPD pose une interdiction de principe des DIA, le législateur suisse a choisi de ne pas reprendre cette interdiction, privilégiant plutôt la transparence et le droit à l'information.

Premièrement, le responsable du traitement doit informer la personne concernée qu'elle fait l'objet d'une telle DIA. Comme toute communication en matière de protection des données, celle-ci doit être effectuée « de manière concise, transparente, compréhensible et facilement accessible »[57]. Le prestataire doit éviter d'utiliser uniquement un jargon juridique. Ainsi, une communication qui indique « vous faites l'objet d'une décision individuelle automatisée » est en principe insuffisante. Au contraire, le responsable du traitement doit expliquer à la personne concernée que la décision a été prise par un processus exclusivement automatisé, c'est-à-dire sans intervention humaine.

Deuxièmement, la doctrine unanime soutient que le responsable du traitement doit également indiquer à la personne concernée ses droits consacrés par l'art. 21 al. 2 LPD[58]. Le prestataire ne peut donc pas se contenter d'informer le client qu'il fait l'objet d'une DIA. Il doit l'informer de ses droits, en particulier du droit d'être informé de la logique sous-jacente et de son droit d'être entendu par un humain.

Ces informations peuvent être communiquées tant avant qu'après la DIA[59]. Néanmoins, une information générale contenue dans la *privacy policy* ne suffit pas (p. ex. « Nous pouvons prendre des décisions individuelles automatisées qui ont des effets juridiques pour vous ou vous affectent de manière significative »). Le responsable du traitement doit bien plus informer les personnes concernées des DIA qu'il utilise[60], par exemple un algorithme qui détecte les transactions suspectes[61].

Contrairement au droit de l'UE qui prévoit un devoir d'informer d'office, il appartient à la personne concernée de requérir auprès du responsable du traitement des explications sur « la logique sur laquelle se base la décision » (art. 25 al. 2 let. f LPD). Par exemple, si le prestataire utilise un *robo advisor*, il pourrait devoir expliquer au client (sur demande) la façon dont, grâce au profil de risque, l'algorithme établit une stratégie de placements appropriée (en indiquant les pondérations des diverses classes d'actifs). Il devrait aussi lui indiquer que la façon dont celle-ci est mise en œuvre et vérifiée par l'algorithme à un certain intervalle régulier[62].

D'une manière semblable au RGPD, la personne concernée peut « faire valoir son point de vue » et exiger une vérification humaine (art. 21 al. 2 LPD)[63]. Le responsable du traitement devrait informer la personne concernée de ses droits[64]. Bien que la LPD ne prévoie pas de délai pour procéder à cette vérification humaine, la doctrine estime qu'un délai de 30 jours

57 Art. 12 par. 1 RGPD. Cf. ég. l'art. 13 OPDo : « Le responsable du traitement communique aux personnes concernées les informations sur la collecte de données personnelles de manière concise, transparente, compréhensible et facilement accessible ».

58 *Rosenthal* (n. 20), N 112 ; BSK DSG-*Henseler/Vasella* (n. 7), Art. 21 N 38. CR LPD-*Flueckiger* (n. 21), Art. 21 N 8 ; *Pärli Kurt/Flück Nathalie,* Art. 21, in : Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (édit.), Datenschutzgesetz (DSG), Bundesgesetz vom 25. September 2020 über den Datenschutz (DSG), 2e éd., Berne 2023.

59 Conseil fédéral (n. 18), p. 6675 ; BSK DSG-*Henseler/Vasella* (n. 7), Art. 21 N 36.

60 BSK DSG-*Henseler/Vasella* (n. 7), Art. 21 N 38.

61 Pour un exemple concret d'une telle clause selon le RGPD, cf. la clause suivante d'ING*: « We are obliged to perform customer and transaction screening to detect potential and actual criminal activity. As a result, we pay particular attention to unusual transactions and to transactions that, by their nature, result in a relatively high risk of fraud, money laundering or terrorism financing. To do this we create and maintain a risk profile for you. If we suspect that a transaction is connected with money laundering or terrorist financing, we are obliged to report this to the authorities. Examples of factors that we take into account that may indicate an increased risk of fraud or money laundering and terrorist financing are:*

- *Changes in a person's normal spending and payment behaviour, such as unexpectedly large amounts being transferred or debited.*
- *Payments to or from suspicious countries, stores or addresses.*
- *Two PIN payments by a single person in two vastly different locations at the same time.*
- *Being listed on any public national or international sanctions lists. »*

62 *Hirsch/Merlino* (n. 7), p. 48.

63 Selon le Conseil fédéral, le but de ce droit est « entre autres d'éviter que le traitement de données soit effectué sur la base de données incomplètes, dépassées ou non pertinentes » (Conseil fédéral [n. 18], p. 6675).

64 Conseil fédéral (n. 18), p. 6675 ; BSK DSG-*Henseler/Vasella* (n. 7), Art. 21 N 36.

pourrait s'appliquer[65]. Ainsi, si une banque refuse d'entrer en relation avec un potentiel client suite à un *onboarding* automatisé, elle devrait l'informer qu'il peut contester cette décision et que celle-ci peut, le cas échéant, être revue par un humain. Le prestataire doit dès lors prévoir un processus interne qui lui permette de respecter le droit d'être entendu de la personne concernée, en particulier désigner un employé compétent qui puisse revoir la DIA contestée.

Enfin, contrairement au droit de l'UE qui impose systématiquement une analyse d'impact de protection des données (AIPD)[66], le responsable du traitement devra procéder à une AIPD uniquement si la mise en œuvre des DIA présente un risque élevé pour les personnes concernées (art. 22 LPD). Cela étant, afin de déterminer si le système de DIA présente un risque élevé, il convient nécessairement de procéder à une première analyse sommaire du risque. Pour établir le risque, il faut multiplier la probabilité d'un événement *(probability)* par l'atteinte *(impact)*[67]. En matière de DIA, cela revient à examiner (1) la probabilité qu'une décision ait un impact négatif sur la personne concernée et (2) l'importance de cet impact. Par exemple, pour le prestataire qui utilise un *robo advisor*, il doit examiner la probabilité que les décisions engendrent des pertes et l'importance de ces pertes pour le patrimoine (total et celui investi) des clients. Si cet examen révèle un risque élevé, il doit établir une AIPD, comme exposé ci-dessus pour le RGPD[68].

IV. Exceptions au régime juridique de la DIA

1. Les exceptions selon l'art. 22 par. 2 RGPD

Les exceptions permettent au responsable du traitement d'adopter une DIA malgré l'interdiction de principe prévue par l'art. 22 par. 1 RGPD[69]. Toute DIA doit donc reposer sur une exception prévue par l'art. 22 par. 2 let. a RGPD, en plus de respecter les principes généraux, en particulier les art. 5 et 6 RGPD[70].

Premièrement, le RGPD autorise les DIA lorsque celles-ci sont « nécessaires » à la conclusion ou à l'exécution d'un contrat (art. 22 par. 2 let. a RGPD). Cette exception trouve son application pratique dans des domaines tels que la gestion de fortune automatisée *(robo advisor)*[71].

La deuxième exception concerne les situations où le droit de l'UE ou des Etats membres le permet (art. 22 par. 2 let. b RGPD). Le législateur allemand a par exemple prévu une telle possibilité en matière de contrats d'assurance[72].

Une dernière exception est le consentement explicite de la personne concernée (art. 22 par. 2 let. c RGPD). Toutefois, le consentement en matière de protection des données est sujet à des exigences strictes : il doit être « libre, spécifique, éclairée et univoque » (art. 4 par. 11 RGPD) et peut être retiré en tout temps (art. 7 par. 3 RGPD), ce qui en fait une base juridique fragile[73]. En pratique, à considérer le *onboarding* comme une DIA[74] et si la première exception ne s'applique pas, le potentiel futur client devrait pouvoir choisir entre un *onbarding* automatisé (et probablement plus rapide) et celui effectué par un être humain afin que son consentement soit libre[75]. Il devrait également disposer d'une information idoine[76].

2. Les exceptions selon l'art. 21 al. 3 LPD

En droit suisse, les exceptions permettent au responsable du traitement de se soustraire à deux obligations : le devoir d'informer et le droit octroyé à la personne concernée de « faire valoir son point de vue » et d'exiger une vérification humaine. En revanche, le

65 Stricte : CR LPD-*Flueckiger* (n. 21), Art. 21 N 9 ; moins stricte : BSK DSG-*Henseler/Vasella* (n. 7), Art. 21 N 46.

66 Cf. *contra Gilliéron Philippe,* in : Métille Sylvain/Meier Philippe (édit), Commentaire Romand, Loi sur la protection des données, Bâle 2023, Art. 22 N 15, qui considère que l'art. 22 al. 1 LPD « est une copie conforme de l'art. 35 par. 1 RGPD ».

67 *Hirsch* (n. 1), p. 79 ; CR LPD-*Gilliéron* (n. 66), Art. 22 N 24 ss.

68 Cf. *supra* III.1.

69 CJUE, C-634/21, OQ contre Land Hessen, en présence de SCHUFA Holding AG, 7 décembre 2023, ECLI :EU :C :2023 :957, par. 52.

70 *Id.*, par. 68.

71 *Hirsch/Merlino* (n. 7), p. 45.

72 § 37 (*Automatisierte Entscheidungen im Einzelfall einschliesslich Profiling)* de la *Bundesdatenschutzgesetz* (BDSG) ; *Philip Scholz,* in : Simitis Spiros/Hornung Gerrit/Spiecker Indra (édit), Datenschutzrecht : DSGVO mit BDSG Grosskommentar, Baden-Baden 2019, Art. 22 DSGVO N 48 ss.

73 *Hirsch/Merlino* (n. 7), p. 46.

74 Selon la portée de l'arrêt de la CJUE dans l'affaire C-634/21 du 7 décembre 2023 (SCHUFA Holding AG), discutée *supra* II.1.

75 *Henseler/Vasella* soulignent expressément qu'un consentement libre nécessite une alternative raisonnable (BSK DSG-*Henseler/Vasella* [n. 7], Art. 21 N 55).

76 Cf. *supra* III.1.

droit d'être informé de la logique sur laquelle se fonde la DIA persiste (art. 25 al. 2 let. f LPD).

En premier lieu, l'exception s'applique si la DIA est en « relation directe » avec le contrat et « la demande est satisfaite » (art. 21 al. 3 let. a LPD). Ainsi, un client qui demande l'octroi d'un crédit en ligne et le reçoit au taux d'intérêt proposé n'a pas besoin d'être informé que l'octroi a fait l'objet d'une DIA[77]. En effet, dans une telle situation, « l'information n'intéresse plus la personne concernée » puisque celle-ci obtient le contrat espéré[78].

En second lieu, le consentement exprès constitue aussi une exception. Ce consentement est similaire au consentement explicite de l'UE[79], et est soumis aux mêmes défis[80]. En particulier, afin que le consentement soit éclairé, la personne concernée doit avoir obtenu au préalable les informations pertinentes relatives aux DIA la concernant[81].

V. Violation des obligations légales

1. Les conséquences en cas de violation de l'art. 22 RGPD

La personne concernée affectée par une violation de l'art. 22 RGPD peut prétendre à des dommages-intérêts en se fondant sur l'art. 82 RGPD, notamment pour indemnisation du « préjudice moral »[82]. Cependant, les montants accordés ne sont généralement pas substantiels[83].

En revanche, les amendes administratives représentent une sanction plus sévère, pouvant atteindre jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial du responsable du traitement, le montant le plus élevé étant retenu (art. 83 par. 5 let. b RGPD)[84]. A notre connaissance, bien qu'aucune amende n'ait été imposée à des entités suisses depuis l'entrée en vigueur du RGPD, la possibilité demeure en raison de l'application extraterritoriale du règlement[85]. Cela étant, la mise en œuvre d'une telle amende contre un responsable du traitement ou sous-traitant suisse soulève quelques problèmes, qui ne seront toutefois pas développés ici[86].

2. Les conséquences en cas de violation de l'art. 21 LPD

Comme dans l'UE, les victimes d'une violation de l'art. 21 LPD peuvent théoriquement réclamer des dommages-intérêts en application de l'art. 41 CO. Néanmoins, la majorité des violations de cette disposition n'entrainera probablement pas de préjudice réparable[87].

Par ailleurs, la nouvelle législation suisse confère au Préposé fédéral à la protection des données et à la transparence (PFPDT) des pouvoirs étendus, incluant la possibilité d'ordonner la suspension du traitement des données ou la suppression des données collectées en violation de la LPD[88]. A notre avis, le PFPDT pourra

77 La condition que « la demande est satisfaite » peut soit vouloir dire que la demande concrète de la personne concernée est satisfaite, soit que la demande aux conditions du marché est satisfaite (BSK DSG-*Henseler/Vasella* [n. 7], Art. 21 N 52 soutiennent la seconde possibilité).

78 Conseil fédéral (n. 18), p. 6675.

79 *Meier Philippe/Tschumy Nicolas,* in : Métille Sylvain/Meier Philippe (édit), Commentaire Romand, Loi sur la protection des données, Bâle 2023, Art. 6 N 93 ss.

80 Sur le consentement éclairé, libre et déterminé, cf. CR LPD-*Meier/Tschumy* (n. 79), Art. 6 N 84 ss.

81 BSK DSG-*Henseler/Vasella* (n. 7), Art. 21 N 54.

82 Concernant ce préjudice moral, cf. *Hirsch* (n. 1), p. 473 : « la CJUE a considéré que l'art. 82 RGPD n'exigeait pas que le dommage moral atteigne un certain degré de gravité afin de pouvoir être réparé. Cela étant, il est nécessaire qu'un tel dommage soit prouvé ; autrement dit, ‹ la simple violation des dispositions [du RGPD] ne suffit pas pour conférer un droit à réparation › [CJUE, C-300/21 (UI contre Österreichische Post AG), 4 mai 2023, par. 51]. Par ailleurs, l'établissement du montant du dommage n'est pas réglé par le RGPD. Partant, chaque État membre est libre de déterminer ‹ les critères permettant de déterminer l'étendue de la réparation due dans ce cadre, sous réserve du respect des (…) principes d'équivalence et d'effectivité › ».

83 Cf. en particulier le tableau, tenu à jour, de l'étude d'avocats Latham (Latham DSGVO-Schadensersatztabelle) : <*https://www.lw.com/de/people/admin/upload/SiteAttachments/Latham-DSGVO-Schadensersatztabelle.pdf*>.

84 Concernant cette amende administrative, cf. *Hirsch* (n. 1), p. 515 ss.

85 Cf. n 4.

86 Cf. *Hirsch* (n. 1), p. 522 ss.

87 Il sera particulièrement compliqué pour la personne concernée de prouver la causalité et son préjudice. En outre, le tort moral est admis en Suisse de manière bien plus restrictive que l'est le préjudice moral au sein de l'Union européenne (cf. *Hirsch* [n. 1], p. 463 ss concernant le tort moral et p. 473 concernant le préjudice moral).

88 Concernant les mesures pouvant être prises par le PFPDT, cf. *Hirsch* (n. 1), p. 500 ss. Cf. ég. *Jacot-Guillarmod Emilie/Thorens Olaf,* Les nouveaux pouvoirs du PFPDT et son rôle dans la poursuite pénale en vertu de la LPD, Jusletter 25 september 2023 ; *Oehri Isabelle/Fanger Reto,* Die Unter-

en particulier ordonner au responsable du traitement d'arrêter purement et simplement son système de DIA en cas de violation crasse de l'art. 21 LPD. Une telle mesure nécessite toutefois de respecter le principe de proportionnalité et ne constituera que l'*ultima ratio*.

La conséquence la plus notable en Suisse est la sanction pénale contre la personne physique responsable de la violation[89]. Cette dernière peut être punie d'une amende de CHF 250 000 au plus si elle omet intentionnellement (ou par dol éventuel) d'informer la personne concernée conformément à l'art. 21 al. 1 LPD (art. 60 al. 1 LPD). La jurisprudence récente semble admettre un seuil relativement bas pour retenir un dol éventuel[90], ce qui pourrait faciliter l'ouverture de procédures pénales contre les personnes responsables. Cela étant, cette sanction nécessite néanmoins une plainte pénale de la part de la personne concernée.

En plus de la responsabilité pénale de la personne compétente de la violation, le supérieur hiérarchique peut aussi se retrouver sanctionné[91]. En effet, l'art. 64 LPD renvoie aux art. 6 et 7 DPA pour les infractions commises dans une entreprise. Or, l'art. 6 al. 2 DPA prévoit que le chef d'entreprise, l'employeur, le mandant ou le représenté qui, intentionnellement ou par négligence et en violation d'une obligation juridique, omet de prévenir une infraction commise par le subordonné, le mandataire ou le représentant ou d'en supprimer les effets, tombe sous le coup des dispositions pénales applicables à l'auteur ayant agi intentionnellement ou par négligence. Partant, les membres de la direction ou du conseil d'administration qui n'exerceraient pas les tâches de haute surveillance pour s'assurer du respect de la LPD, à tout le moins dans ses grandes lignes, peuvent voir leur responsabilité pénale engagée en cas de violation du devoir d'informer au sens de l'art. 60 al. 1 LPD[92].

VI. Perspectives

En Suisse, trois éléments centraux détermineront la mise en œuvre concrète des devoirs légaux en cas de DIA :

1. Les personnes concernées vont-elles exercer leurs droits, en particulier leur droit d'être entendu et celui d'avoir accès à la logique sous-jacente ?
2. Le PFPDT va-t-il exercer son rôle de surveillant et ouvrir, le cas échéant, des procédures d'*enforcement* ? Le cas échéant, quelle sera la collaboration entre cette autorité et la FINMA[93] ?
3. Les personnes concernées dont les droits sont violés vont-elles porter plainte ? Le cas échéant, les autorités pénales compétentes vont-elles condamner les personnes responsables ?

Si le responsable du traitement respecte son devoir d'informer en cas de DIA, certaines personnes concernées exerceront très probablement leur droit d'être entendu et, sur la base du droit d'accès, demanderont à connaître la logique sous-jacente. L'exercice de ces droits devrait être gratuit, ce qui laisse supposer qu'ils seront bien utilisés en pratique. Les prestataires de services bancaires et financiers devraient se préparer à réagir à de telles demandes. S'ils ne respectent pas ces droits, la personne concernée pourrait dénoncer le prestataire à la FINMA et au PFPDT.

Une fois informées d'un tel cas, quelle sera la réaction de ces deux autorités ? Probablement, les violations mineures ne seront pas leur priorité. Cela étant, selon la taille du prestataire et en fonction du nombre de personnes auxquelles la prestation en cause est offerte, les autorités pourraient réagir fermement afin d'établir un précédent. Partant, même si la probabilité peut sembler faible, les conséquences de l'ouverture d'une procédure par l'une (ou les deux) de ces autorités pourraient être importantes, compte tenu de leurs pouvoirs.

En outre, la personne concernée pourrait, en plus de la dénonciation aux autorités, déposer une plainte

suchung von Datenschutzverstössen durch den EDÖB, Jusletter 25 september 2023.

89 Cf. *Pahud Joël/Pittet Sébastien*, Les infractions pénales de la loi sur la protection des données, Jusletter 25 septembre 2023, N 76 ss.

90 Cf. en particulier l'arrêt du Tribunal fédéral 6B_899/2021 du 26 janvier 2023, rendu à la suite d'une audience publique mais non destiné à publication (sur cet arrêt, cf. ég. LawInside.ch/1297/ et cdbf.ch/1273/).

91 *Métille Sylvain*, in : Métille Sylvain/Meier Philippe (édit), Commentaire Romand, Loi sur la protection des données, Bâle 2023, Art. 64 N 12.

92 CR LPD-*Métille* (n. 91), Art. 64 N 14. Pour une application récente de l'art. 6 al. 2 DPA, cf. l'arrêt du Tribunal fédéral 6B_1176/2022, 6B_1198/2022 du 5 décembre 2023 (violation par négligence de l'obligation de communiquer au sens de l'art. 37 LBA), commenté par *Villard Katia*, Lutte contre le blanchiment : Violation de l'obligation de communiquer et responsabilité du Conseil d'administration, publié le 8 janvier 2024 par le Centre de droit bancaire et financier, <*https://cdbf.ch/1317/*>.

93 Cf. *Hirsch* (n. 1), p. 510 ss.

pénale. L'autorité pénale compétente devra en principe instruire la cause[94]. Elle pourra en particulier ouvrir une procédure tant contre la personne physique qui a concrètement violé le devoir d'informer que contre le dirigeant qui devait surveiller le respect de la LPD[95]. En raison des lourdes conséquences découlant de l'ouverture d'une procédure pénale, ce risque n'est pas négligeable.

Enfin, des révisions législatives sont déjà en cours d'élaboration. Certains parlementaires suisses sont conscients que le champ d'application de la DIA est limité, notamment en raison du critère « exclusivement automatisé ». La Conseillère nationale *Min Li Marti* a déposé une motion afin que « tout recours à l'IA dans un système ou une application soit clairement signalé, à quelque niveau que ce soit »[96]. Bien que le Conseil fédéral en propose le rejet, il a indiqué être en train de dresser un état des lieux relatif à la règlementation de l'intelligence artificielle, lequel « examinera aussi dans quelle mesure il est approprié pour la Suisse, en ce qui concerne l'obligation de déclaration des systèmes d'IA, d'avoir une règlementation qui va au-delà des règles déjà prévues dans la [LPD] »[97]. De son côté, le Groupe des Verts-e-s a déposé une initiative parlementaire le 15 juin 2023 visant à ajouter un art. 21[bis] à la LPD, lequel viserait précisément le devoir d'informer en cas d'utilisation de l'intelligence artificielle[98]. En fonction des conclusions de l'état des lieux que prépare actuellement le Conseil fédéral, cette initiative pourrait être intégrée à une révision législative plus large liée à l'intelligence artificielle.

Enfin, au sein de l'UE, le futur règlement européen sur l'intelligence artificielle (Loi sur l'IA) pourrait aussi concerner l'automatisation des services financiers[99]. Ce règlement s'appliquera en plus de l'art. 22 RGPD[100]. Certaines prestations automatisées pourront donc se trouver dans le champ d'application des deux règlements. En particulier le *credit scoring* sera considéré comme un système d'intelligence artificielle à haut risque[101]. En revanche, la détection de fraudes ne sera pas considérée comme un système à haut risque[102]. En outre, son effet extraterritorial, semblable à celui du RGPD, influencera certainement la pratique en Suisse[103]. Même si cette Loi sur l'IA est sur le point d'être adoptée, le texte final n'a pas encore été officiellement publié[104].

VII. Conclusion

L'intelligence artificielle pose de nombreux défis. Cette contribution a présenté son application dans les services bancaires et financiers en cas de décision individuelle automatisée (DIA ; art. 21 LPD et art. 22 RGPD). Nos conclusions sont résumées ci-dessous.

Premièrement, l'arrêt de la CJUE dans l'affaire SCHUFA Holding AG élargit la portée de la notion de « décision » au sens du RGPD, impliquant que même la transmission d'un score de solvabilité à un tiers peut constituer une DIA. Même si elle a été prise dans un contexte précisément visé par le considérant 71 du RGPD, cette jurisprudence pourrait s'étendre à de nombreuses démarches qui n'étaient, jusqu'à alors, pas considérés comme des DIA, telles que les évaluations de certaines caractéristiques. Tout prestataire effectuant une évaluation automatisée, laquelle permet à un partenaire contractuel de prendre une décision, devrait désormais examiner attentivement s'il doit se conformer aux devoirs légaux prévus en cas de DIA.

94 Sur la portée du principe *in dubio pro duriore*, cf. ATF 143 IV 241 (résumé in : LawInside.ch/500/).

95 Cf art. 6 al. 1 et al. 2 DPA *cum* art. 64 LPD ; *Pahud/Pittet* (n. 89), N 80 s.

96 Motion 23.3806 de Mme *Min Li Marti* déposée le 15 juin 2023.

97 Avis du Conseil fédéral du 30 août 2023 répondant à la motion 23.3806 de Mme *Min Li Marti* déposée le 15 juin 2023.

98 Initiative parlementaire 23.438 du Groupe des Verts-e-s déposée le 15 juin 2023.

99 *Caballero Cuevas Yannick*, Union européenne : Le projet européen de règlement sur l'IA : *Quid* des services financiers ?, publié le 30 avril 2021 par le Centre de droit bancaire et financier, <*https://cdbf.ch/1181/*>.

100 *von Lewinski* (n. 8), Art. 22 DGSVO N 1.2.

101 Annexe III, Art. 5 let. b Loi sur l'IA. Cf. ég. considérant 37 de la Loi sur l'IA.

102 *Id.*

103 Art. 2 Loi sur l'IA.

104 Parlement européen, Loi sur l'intelligence artificielle : accord sur des règles globales pour une IA digne de confiance, 9 décembre 2023 (<*https://www.europarl.europa.eu/news/fr/press-room/20231206IPR15699/loi-sur-l-intelligence-artificielle-accord-sur-des-regles-globales*>). Une version presque définitive a néanmoins été dévoilée en ligne fin janvier 2024, ce qui nous a permis d'en prendre connaissance (cf. ég. *Dal Molin Luca/Silberstein-Loeb Jonathan*, Leaked Draft of EU AI Act Sheds Light on Proposed Regulation, 26 janvier 2024, <*https://www.homburger.ch/en/insights/leaked-draft-of-eu-ai-act-sheds-light-on-proposed-regulation*>).

Deuxièmement, chaque responsable du traitement devrait examiner le degré d'intervention humaine *(human in the loop)* en cas de proposition de décision automatisée. Si l'intervention humaine respecte les cinq conditions susmentionnées, la décision revue par l'humain ne constitue pas une DIA.

Troisièmement, l'impact des décisions automatisées sur les personnes concernées doit être significatif pour que la décision soit qualifiée de DIA. Bien que cette exigence d'impact ajoute une couche de complexité dans l'évaluation des conséquences juridiques des DIA, elle permet aussi d'écarter l'application de ses règles. En pratique, le prestataire peut avoir intérêt de considérer toutes ses décisions automatisées comme des DIA, afin de ne pas devoir examiner si chaque décision déploie des effets significatifs sur les personnes concernées.

Par ailleurs, alors que le RGPD impose une interdiction de principe avec des exceptions spécifiques, le droit suisse se concentre davantage sur le droit à l'information. De manière similaire, le RGPD et la LPD imposent au prestataire une certaine transparence, en particulier d'informer la personne concernée de la logique de la DIA, et de respecter le droit d'être entendu par un humain. Concrètement, le prestataire devrait prévoir l'explication de la logique de la DIA et organiser un processus afin de respecter ce droit d'être entendu.

Trois éléments pourraient influencer grandement la mise en œuvre en Suisse des devoirs légaux découlant de l'existence d'une DIA. Premièrement, elle dépendra de l'exercice effectif des droits par les personnes concernées, notamment leur droit d'être entendu et d'accéder à la logique sous-jacente des DIA. Deuxièmement, la surveillance exercée par le PFPDT et la FINMA, et leur collaboration en la matière, seront déterminantes. Troisièmement, la mise en œuvre sera influencée par la réaction des personnes concernées face aux potentielles violations de leurs droits, notamment si elles procèdent à des dénonciations auprès du PFPDT et de la FINMA, voire si elles déposent des plaintes pénales.

Enfin, l'impact potentiel de la Loi sur l'IA de l'UE et les évolutions législatives en Suisse indiquent que le cadre juridique de l'intelligence artificielle et des DIA continuera d'évoluer. Les prestataires de services financiers doivent donc rester vigilants et réactifs face à ces changements législatifs, en assurant la conformité actuelle, voire en anticipant les implications de ces évolutions sur leurs processus utilisant l'intelligence artificielle.