



جامعة الشارقة
UNIVERSITY OF SHARJAH

University of Sharjah Journal of Law Sciences

A Refereed Scientific journal



Vol. 23, No. 1
Ramadan 1446 A.H. / March 2026 A.D.

ISSN : 2616-6526

La prise de décision automatisée Une analyse comparative entre le RGPD européen et le Décret-loi fédéral émirati n°45 de 2021

Laroussi Chemlali⁽¹⁾

Reçu le : 21-11-2024

Accepté le : 16-01-2025

Résumé:

A l'ère du numérique, le recours croissant aux systèmes de décision automatisée par les entreprises et les institutions publiques soulève des enjeux majeurs en matière de protection des données personnelles et des droits fondamentaux. Cette étude propose une analyse comparative de l'encadrement juridique de la prise de décisions automatisées entre le Règlement Général sur la Protection des Données (RGPD) européen et le Décret-loi fédéral émirati n°45 de 2021 concernant la protection des données personnelles, mettant en lumière les différentes approches adoptées par ces deux textes pour réguler l'usage des systèmes automatisés de prise de décision. La présente recherche examine en profondeur les convergences et divergences entre ces deux cadres réglementaires, notamment en ce qui concerne les garanties offertes aux personnes concernées, les obligations imposées aux responsables de traitement dans ce contexte. Pour ce faire, nous avons commencé par définir les contours de la notion de prise de décision automatisée et les défis qu'elle pose, avant d'étudier les garanties et obligations prévues par le RGPD européen et le Décret-loi émirati n°45.

Mots clés: Décision automatisée, Protection des données personnelles, RGPD, Décret-loi fédéral n°45/2021.

(1) Faculté de droit - Université d'Ajman (Ajman - Émirats arabes unis)
l.chemlali@ajman.ac.ae

Introduction

A l'ère du numérique, les entreprises et les institutions publiques ont de plus en plus recours à des systèmes de décision automatisée. Ces outils, devenus incontournables, s'appuient le plus souvent sur l'intelligence artificielle et des algorithmes sophistiqués pour optimiser les processus décisionnels. Aujourd'hui, la prise de décision automatisée est déployée dans de nombreux secteurs. Cela inclut des domaines tel que la santé (prédiction des maladies, diagnostic médical assisté, etc.), la finance (score de crédit, détection de fraudes), les ressources humaines (présélection des CV, planification des entretiens, appariement des candidats - emploi, etc.), le marketing (personnalisation de contenu), les transports (systèmes de navigation autonomes), et la sécurité publique (prédiction de crimes).

Cependant, cette dépendance croissante à l'égard des systèmes automatisés soulève des questions cruciales en matière de protection des données personnelles et de respect de la vie privée des citoyens. En effet, le recours à des systèmes décisionnels automatisés implique souvent la collecte et le traitement d'un volume considérable de données personnelles. Ces données pourraient inclure des détails sur la vie professionnelle, personnelle, ou même sur la santé des individus.

En réponse à ces problématiques émergentes, diverses initiatives législatives ont émergé dans le monde entier. Parmi les plus significatives figurent d'une part le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD, 2016), pierre angulaire de la protection des données en Europe depuis 2018, et d'autre part le Décret-loi fédéral

émirati n°45 de 2021 relatif à la protection des données personnelles (Décret-loi n°45, 2021).

Cette étude entreprend une analyse comparative des approches adoptées par le RGPD et le Décret-loi émirati en matière de prise de décision automatisée. L'objectif est d'examiner en profondeur les similitudes et les différences entre ces deux cadres réglementaires. La recherche se penche sur la manière dont chacun des deux textes définit et encadre ces processus, les garanties qu'il confère aux individus, ainsi que les obligations qu'il impose aux responsables du traitement des données.

Pour ce faire, l'étude sera structurée en deux parties : d'abord, une exploration du concept de décision automatisée et ses enjeux (I), puis une étude comparative détaillée du RGPD européen et du Décret-loi émirati n°45, examinant leurs convergences et divergences en matière de protection individuelle et d'obligations des responsables de traitement (II).

I. Comprendre les Décisions Automatisées : Cadre Conceptuel et Défis

Cette première partie s'articulera autour de deux axes : d'une part, la définition et la typologie des décisions automatisées (A), d'autre part, l'analyse des défis spécifiques de la prise de décision automatisée (B).

A. Définition et Typologie des Décisions Automatisées

Dans un premier temps, l'étude abordera la définition de la prise de décision automatisée (1). Ensuite, elle traitera des différents types de prise de décision automatisée en fonction du degré d'implication humaine (2).

1. La définition de la prise de décision automatisée

Le concept de la prise de décision automatisée n'a pas été définie dans le RGPD, ni dans le Décret-loi fédéral n°45 de 2021 des Émirats Arabes Unis. Les deux textes se sont limités à prévoir une interdiction de principe des décisions fondées exclusivement sur le traitement automatisé des données personnelles.

Pour définir la prise de décision automatisée, différentes approches existent actuellement dans le débat public et la littérature académique. Selon les lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 016/679, élaborées par le groupe « Article 29 » (G29), et désormais remplacé par le Comité Européen sur la Protection des Données (CEPD) depuis l'entrée en vigueur du RGPD, la décision individuelle automatisée désigne un processus qui consiste à prendre une décision à l'égard d'une personne exclusivement sur la base d'un traitement automatisé de données personnelles, sans intervention humaine significative directe dans ce processus (G29, 2018, p. 8). Dans le même sens, dans un rapport intitulé 'Automating Society – Taking Stock of Automated Decision-Making in the EU', l'organisation AlgorithmWatch définit la prise de décision automatisée comme 'un ensemble de procédures dans lesquelles les décisions sont initialement - partiellement ou totalement - déléguées à une autre personne ou entité commerciale, qui à son tour utilise des modèles de prise de décision exécutée automatiquement pour effectuer une action. Cette délégation – non pas de la décision elle-même, mais de l'exécution – à un système basé sur les données et contrôlé par un algorithme, est ce qui mérite notre attention' (AlgorithmWatch, 2019). Ainsi définie, la notion de décision automatisée englobe un large éventail de systèmes de prise de décision allant des plus simples, basés sur des

algorithmes basiques fondés sur des règles prédéfinies, aux plus complexes, utilisant l'apprentissage profond ou bien les réseaux neuronaux.

Cette conception inclusive se démarque de l'approche adoptée par les experts en IA, qui distinguent entre la 'décision automatisée', la 'décision autonome', et la 'décision algorithmique' (Brkan & Bonnet, 2020). Bien que l'objectif soit le même dans les trois cas, à savoir effectuer des actions sans intervention humaine dans le processus, ils diffèrent considérablement dans leurs caractéristiques. Un processus automatisé est un processus logiciel ou matériel qui exécute une séquence d'actions prédéfinie sans intervention humaine. Il en découlerait que les décisions seraient facilement prédictibles. En revanche, dans le processus de décision autonome, la machine possède une grande autonomie. Dans ce contexte, l'humain se contente de déterminer un objectif général, laissant ensuite à la machine/l'algorithme le soin de déterminer les stratégies et les étapes les plus appropriées pour atteindre cet objectif. Quant à la décision algorithmique, elle signifie simplement qu'un algorithme a participé au processus décisionnel. Elle englobe donc à la fois les décisions autonomes et automatisées. Cela inclut les décisions prises de manière autonome ainsi que celles prises de façon automatisée. En d'autres termes, la prise de décision algorithmique englobe tout système où un algorithme joue un rôle, quel que soit le niveau d'autonomie accordé.

2. Typologie des décisions automatisées

Les décisions individuelles automatisées peuvent être classées en trois types en fonction du niveau d'implication humaine : celles avec humain 'dans la boucle', celles avec humain 'sur la boucle' et celles avec humain 'hors la boucle' (Ivanov, 2023). Dans les systèmes de prise de décision où l'humain est 'dans la boucle', l'algorithme fait des recommandations,

mais c'est à l'humain que revient la décision finale. Cette méthode est adaptée aux décisions complexes qui nécessitent un jugement humain et des considérations éthiques, garantissant que la perspicacité humaine est intégrée à la décision finale. A titre d'exemple, dans la finance, des algorithmes sont souvent utilisés afin d'aider à détecter les transactions frauduleuses. Ces transactions sont ensuite examinées par les analystes humains qui prennent la décision finale à leur égard (Rahwan et al., 2019).

Dans le système de prise de décision où l'humain est 'sur la boucle', l'algorithme est habilité à prendre des décisions, mais les humains supervisent le processus et peuvent passer outre s'ils le jugent nécessaire. Ce système combine l'efficacité de l'automatisation avec la nécessité d'une supervision humaine, ce qui le rend idéal dans les circonstances complexes nécessitant des décisions rapides tout en préservant la valeur du jugement humain (Fischer et al., 2012). C'est le cas des algorithmes de tarification dynamique utilisés par les compagnies aériennes et les hôtels afin d'optimiser leurs bénéfices en ajustant leurs prix en temps réel, en fonction des fluctuations de l'offre et de la demande. Ces algorithmes analysent une multitude de données, telles que la demande actuelle, la concurrence, la saisonnalité, ou bien les événements spéciaux, afin de déterminer le prix optimal. Toutefois, en dépit de leur performance, ces algorithmes ne sont pas toujours en mesure de considérer tous les facteurs susceptibles d'influencer les prix. C'est pourquoi les décisionnaires peuvent toujours intervenir et modifier, à la hausse ou à la baisse, les prix recommandés par l'algorithme (Spann et al., 2024).

Enfin, dans le système où l'humain est « hors de la boucle », l'humain est entièrement exclu du processus décisionnel. Dans de tels systèmes, les décisions se font de manière autonome sur la base de règles et d'algorithmes

prédéfinis, dépourvus de l'adaptabilité et de la compréhension nuancée que permet l'intervention humaine. Le trading à haute fréquence en est un parfait exemple : des algorithmes passent des ordres d'achat et de vente sur les marchés financiers à une vitesse ultra-rapide, de l'ordre de la nanoseconde, sans intervention humaine directe (Borch, 2016).

B. Les défis de la prise de décision automatisée

Bien qu'elle offre de nombreux avantages en termes d'efficacité, de rapidité, et de la capacité à traiter des grandes quantités de données en un bref laps de temps, la prise de décision automatisée soulève également des défis et des risques importants qu'il convient d'examiner attentivement.

1. Les Biais et Discriminations

Un des principaux défis que pourrait poser la prise de décision automatisée est celui des biais et des discriminations. Ainsi, l'efficacité des décisions automatisées repose en grande partie sur la qualité et l'exhaustivité des données sous-jacentes. Ces données servent à l'entraînement de l'algorithme dans sa prise de décision. En conséquence, lorsque les données d'entraînement sont biaisées, inexactes, ou reflètent des préjugés sociaux, ces imperfections pourraient se répercuter dans les décisions prises par l'algorithme (Besse et al., 2018). Cela peut engendrer des évaluations discriminatoires, des recommandations biaisées, ou des prises de décision inéquitables, avec des conséquences potentiellement graves pour les individus et la société. Un exemple pertinent pour illustrer ce risque est celui des algorithmes utilisés par les agences de notation de crédit pour évaluer la solvabilité d'un emprunteur (Prince & Schwarcz, 2019). Le rôle de ces algorithmes est crucial dans le système financier, dans la mesure où ils influencent considérablement les décisions des prêteurs et impactent de

manière significative les conditions de crédit octroyés aux emprunteurs. Ils prennent en compte divers facteurs, tels que les antécédents de paiement, l'historique de crédit, le niveau d'endettement ainsi que d'autres éléments pour déterminer le risque associé à l'octroi d'un emprunt. Plus la notation de crédit est élevée, plus l'emprunteur est considéré comme fiable et apte à rembourser un prêt, et inversement (Hurley & Adebayo, 2016).

Toutefois, des préoccupations subsistent quant aux biais éventuels dans les systèmes de notation de crédit, qui sont susceptible de conduire à des décisions discriminatoires ou injustes. En effet, ces biais peuvent provenir de divers facteurs, notamment des données historiques déséquilibrées, de variables sensibles telles que l'origine ethnique ou le sexe, ou de modèles de notation opaques. Ces biais peuvent défavoriser certains groupes de personnes en fonction de leur âge, de leur sexe, ou de leur origine sociale ou ethnique, en limitant leur accès au crédit ou en leur imposant des conditions d'emprunt moins favorables. Une étude récente de la Réserve fédérale américaine corrobore cette réalité. Elle révèle que les candidats appartenant aux minorités noires, hispaniques et amérindiennes affichent souvent des scores de crédit significativement plus bas, et ont moins de chances que les candidats blancs d'obtenir l'approbation des systèmes de souscription automatisés gouvernementaux, et ce, malgré le fait que ces systèmes ne prennent pas explicitement en compte le facteur racial (Bhutta et al., 2022).

2. La protection des données personnelles

Les systèmes de prise de décision automatisée s'appuient sur une immense quantité de données personnelles pour fonctionner efficacement, ce qui suscite d'importantes préoccupations quant à la protection de ces

données (Christodoulou & Limniotis, 2024). Les individus peuvent ne pas être conscients de la manière dont leurs données sont utilisées ou de l'étendue de leur analyse. Les algorithmes d'apprentissage automatique, en particulier, sont capables d'analyser et d'apprendre des expériences et des environnements passés, ce qui leur permet de générer des prédictions et des inférences à partir des données d'entrée. Ces «données inférées» peuvent révéler des aspects inattendus de la vie privée des personnes concernées dont elles n'avaient pas l'intention de partager initialement. A titre d'exemple, l'analyse de leurs achats en ligne peut dévoiler des informations sur leurs opinions politiques, leur santé, ou leur situation financière, sans qu'ils n'aient jamais consciemment divulgué ces informations (Wiedemann, 2018).

3. L'explicabilité et de l'interprétabilité des décisions automatisées

Un autre défi majeur est celui de l'explicabilité(1) et d'interprétabilité(2) des décisions automatisées. En effet, les algorithmes complexes utilisés, notamment ceux basés sur l'apprentissage profond, fonctionnent souvent comme des «boîtes noires», rendant leur raisonnement opaque et difficile à déchiffrer, même pour ceux qui les ont conçus. Pourtant, l'intégration d'une certaine forme d'explicabilité et d'interprétabilité dans ces systèmes de décisions automatisées s'avère indispensable pour de multiples raisons, notamment quand il s'agit de secteurs sensibles tels que la santé, les finances ou la justice. Cela inclut la nécessité de rassurer les utilisateurs sur le bon fonctionnement du système ; à évaluer ses vulnérabilités ou à

- (1) Dans le contexte des décisions automatisées, l'explicabilité désigne la capacité de mettre en relation et de rendre compréhensible les éléments pris en compte par un système de prise de décision automatisée pour arriver à une décision ou un résultat.
- (2) L'interprétabilité se réfère ici à la capacité des individus concernés à comprendre et à expliquer facilement les causes d'une décision automatisée.

valider ses résultats ; de se protéger contre les biais ; de se conformer aux normes réglementaires, et de répondre aux attentes sociétales concernant la participation des individus dans le processus décisionnel.

4. L'imputabilité de la responsabilité

La complexité des algorithmes soulève un véritable dilemme quant à l'imputabilité de la responsabilité (Bensamoun & Loiseau, 2017). En effet, lorsqu'une décision prise sur la base d'un traitement algorithmique produit des effets préjudiciables, comme par exemple la discrimination contre un individu en raison de ses conditions sociales, il est souvent ardu de déterminer qui doit en assumer la responsabilité. Est-ce l'algorithme lui-même, les développeurs qui ont conçu et entraîné l'algorithme, ou bien les organisations qui utilisent ces algorithmes dans leurs processus de décision qui devraient être prises pour responsables ? Cette question se complexifie encore plus quand il s'agit d'algorithmes d'apprentissage automatique, souvent considérés comme des boîtes noires, qui sont capables d'évoluer de manière autonome au fil du temps (Castets-Renard, 2019). Ce faisant, la responsabilité se dilue entre les différents acteurs impliqués dans le processus de décision automatisée, allant du concepteur de l'algorithme à l'entreprise qui le déploie. Cette situation rend l'imputabilité de responsabilité particulièrement difficile et est susceptible de créer un écosystème intriqué où, en cas de problème, chaque partie prenante pourrait se décharger de la faute en pointant de doigt les autres intervenants impliqués. Les concepteurs d'algorithmes peuvent se défendre en arguant qu'ils ont fourni un outil neutre, tandis que les entreprises qui les déploient peuvent affirmer n'avoir fait qu'utiliser une technologie existante. Entre ces deux pôles, on trouve un éventail d'acteurs intermédiaires, à savoir les data scientists qui veillent à l'entraînement des modèles, les ingénieurs qui

les intègrent dans les systèmes de décision, les managers qui décident de leur utilisation, et même les utilisateurs finaux qui interprètent les résultats (Castets-Renard, 2016).

II. Les exigences relatives à la prise de décision automatisée

Après avoir défini la notion de prise de décision automatisée et ses défis, il convient d'examiner les exigences légales qui y sont associées. Cette analyse se concentrera sur deux aspects : les droits conférés aux personnes concernées par les décisions automatisées (A) et les obligations incombant aux responsables du traitement (B).

A. Les droits de la personne concernée par une prise de décision automatisée

Le RGPD ainsi que le Décret-loi fédéral n°45 confèrent aux individus plusieurs droits importants en matière de prise de décision automatisée. Ces législations incluent des droits généraux de protection des données, tels que le droit à l'information, le droit d'accès, le droit de rectification et le droit de limiter le traitement, qui ne seront pas détaillés ici. En outre, elles prévoient des droits spécifiques relatifs à la prise de décision automatisée, permettant aux individus de mieux comprendre et contrôler l'impact des technologies automatisées sur leurs données personnelles et leurs droits, que nous examinerons en détail ci-après.

1. Le Droit de ne pas faire l'objet d'une prise de décision automatisée

Tant le RGPD que le Décret-loi fédéral n°45 de 2021 garantissent à toute personne le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé. Des exceptions sont néanmoins apportées à ce droit, mais elles ne sont applicables que lorsqu'elles sont assorties de

garanties appropriées.

1.1. Interdiction de principe de certaines décisions automatisées

Tant le RGPD que le Décret-loi fédéral n°45 de 2021 garantissent à toute personne le droit de ne pas faire l'objet d'une décision fondée sur un traitement automatisé, mais avec des nuances importantes. L'article 22 du RGPD stipule que : « 1. La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire », tandis que l'article 18 du Décret-loi fédéral n°45 de 2021 énonce que « 1. La personne concernée a le droit de s'opposer à toute décision résultant d'un traitement automatisé, y compris le profilage, en particulier les décisions qui ont un impact juridique ou qui affectent négativement la personne concernée ».

La lecture comparative des deux textes fait apparaître à la fois des points de divergence et de convergence.

S'agissant en premier lieu des points de divergence, le tout premier à relever ici, c'est la différence d'approche entre le RGPD et le Décret-loi n°45 de 2021 concernant le droit de ne pas faire l'objet d'une décision fondée sur un traitement automatisé. Le RGPD adopte une perspective plus restrictive en limitant l'interdiction aux décisions « exclusivement » automatisées. Cela signifie que l'interdiction s'applique uniquement aux décisions prises sans aucune intervention humaine dans le processus de décision. Autrement dit, pour qu'une décision soit considérée comme exclusivement automatisée, et donc interdite aux termes de l'article 22 du RGPD, il ne doit pas y avoir d'intervention humaine réelle et substantielle, et le contrôle humain ne doit pas se limiter à « un simple geste symbolique »

(Article 29 Data Protection Working Party, 2018, p 21; Davis, & Schwemer, 2023; Lazcoz, & De Hert, 2023). En revanche, le Décret-loi fédéral n°45 opte pour une approche plus large et inclusive, englobant « toute décision » issue d'un traitement automatisé. Cette formulation élargie signifie que l'interdiction ne se limite pas aux décisions totalement automatisées, mais englobe également les décisions partiellement automatisées.

L'autre point de divergence entre le Décret-loi fédéral n°45 et le RGPD réside dans la formulation du droit des individus au regard des décisions automatisées (Chemlali et al., 2023). En effet, le Décret-loi adopte une posture plus proactive en mettant en place « un droit de s'opposer » aux décisions automatisées. Cette formulation implique une initiative ou bien une démarche concrète de la part de la personne concernée vis-à-vis des décisions automatisées. Elle met en avant la nécessité pour la personne concernée d'entreprendre des actions actives pour contester ou refuser a posteriori une décision automatisée la concernant. Cette perspective permet aux organisations de continuer à utiliser les processus de décision automatisés, à condition qu'elles disposent de mesures appropriées pour gérer les oppositions des personnes concernées.

En revanche, malgré la formulation ambiguë de l'article 22 (1) RGPD (Tosoni, 2021), il existe une quasi-unanimité sur le fait que cet article instaure une interdiction générale de prendre des décisions fondées exclusivement sur un traitement automatisé, et non seulement un droit de s'opposer à ces décisions comme il est le cas dans le Décret-loi fédéral n°45 (Article 29 Data Protection Working Party, 2018, p 21 ; Thouvenin et al., 2022 ; Kaminski & Urban, 2021 ; Mendoza & Bygrave, 2017). Cela signifie que le RGPD offre à la personne concernée une protection par défaut, dans la mesure où l'interdiction de décisions fondées exclusivement

sur un traitement automatisé s'applique d'une manière systématique, sans nécessiter que la personne concernée prenne une action particulière.

S'agissant, en second lieu, des points de convergence, aucun des deux textes sujets de notre étude comparative ne précise ou donne des indicateurs permettant de déterminer quand est-ce qu'une décision automatisée peut être qualifiée comme ayant des « effets juridiques » à l'égard de la personne concernée, ou est susceptible de l'affecter « négativement » ou bien « de manière significative de façon similaire »

Dans ses lignes directrices relatives à la prise de décision individuelle automatisée et au profilage, le G29 est venu préciser les contours de ces deux termes. Pour ce qui des décisions « produisant des effets juridiques », cela inclut toute décision pouvant influencer les droits légaux dont jouit une personne tels que le droit d'association, le droit de vote ou le droit d'intenter une action en justice. Cela peut également englober les droits acquis en vertu d'un contrat, comme par exemple la décision automatisée entraînant l'annulation d'un contrat, le refus de l'attribution d'un avantage social accordé par la loi, le refus d'admission dans un pays ou le refus de citoyenneté (G29, 2018, p.24).

Pour ce qui est des décisions affectant la personne concernée « de manière significative de façon similaire », les lignes directrices expliquent que pour répondre à ce critère, « les effets du traitement doivent être suffisamment conséquents ou importants pour être pris en considération » (G29, 2018, p.24). Elles soulignent que la décision doit être de nature à affecter de manière significative la situation, le comportement ou les choix des personnes concernées; avoir un impact durable ou permanent sur elles ; ou, dans les cas les plus extrêmes, conduire à leur exclusion ou à leur discrimination

(G29, 2018, p. 24). Bien qu'il soit difficile d'établir une liste exhaustive de ce qui serait suffisamment significatif pour que le régime de l'article 22 s'applique, certaines décisions pourraient potentiellement être incluses dans cette catégorie : celles qui influencent la situation financière d'une personne, comme son éligibilité au crédit ; celles qui affectent l'accès aux services de santé ou de l'éducation ; et celles qui privent une personne d'une opportunité d'emploi ou la désavantagent gravement (G29, 2018, p. 24).

1.2. Exceptions au principe d'interdiction des décisions automatisées

Le RGPD ainsi que le Décret-loi fédéral n°45 prévoient trois situations dans lesquelles le recours à des décisions automatisées est autorisé. La décision automatisée est permise si la loi l'autorise, par exemple pour lutter contre la fraude ou bien l'évasion fiscale. La prise de décision automatisée peut également être autorisée si elle s'avère indispensable à la conclusion ou à l'exécution d'un contrat entre la personne concernée et le responsable du traitement. Cela peut être pertinent dans de nombreuses situations. C'est le cas, par exemple, des décisions nécessaires pour minimiser les risques d'impayés, réduire les risques liés aux erreurs humaines ou encore accélérer le processus de décision. Dans tous les cas, le responsable du traitement doit être en mesure de prouver la nécessité de ce type de traitement, en tenant compte de l'existence potentielle d'autres alternatives plus respectueuses pour la vie privée. Si des moyens tout aussi efficaces mais moins intrusifs sont disponibles pour parvenir aux mêmes fins, alors le traitement en question ne pourrait pas être qualifié de "nécessaire" (G29, 2018, p. 26). Enfin, l'interdiction peut être levée lorsque la prise de décision automatisée est fondée sur le consentement de la personne concernée. Un consentement valide doit être spécifique, éclairé, sans ambiguïté et exprimé par une action affirmative claire (opt-in). Par conséquent, le consentement

ne peut pas être accordé par des cases pré-cochées, le silence ou l'inactivité (Chemlali et al., 2023). Cependant, dans certains contextes spécifiques, retenir le consentement comme base légale pour la prise de décisions automatisées peut s'avérer problématique. L'un de ces cas concerne les décisions automatisées dans le domaine du recrutement ou celles prises dans le cadre des relations de travail, où la validité du consentement peut être remise en question (Lukács & Váradi, 2023).

La principale difficulté dans ce contexte réside dans la démonstration du caractère libre du consentement. En effet, la relation de dépendance inhérente au milieu professionnel soulève des interrogations quant à la véritable liberté du salarié ou du candidat à l'emploi de donner ou de refuser son consentement. Il existe une asymétrie de pouvoir entre l'employeur et l'employé (ou le candidat quand il s'agit d'une procédure de recrutement) qui peut influencer la décision de consentir. D'ailleurs, tant le Groupe de travail Article 29 dans son avis sur le traitement des données sur le lieu de travail (G29, 2017), que le Comité Européen de la Protection des Données dans ses lignes directrices sur le consentement au sens du RGPD (CEPD, 2020), ont souligné cette problématique. Ils ont fait remarquer qu'au vu de la dépendance résultant de la relation employeur/employé, il est peu probable qu'un employé puisse refuser de donner son consentement sans craindre des conséquences négatives. Cette situation met en doute la validité du consentement comme base légale du traitement des données personnelles des employés.

2. Le droit à une intervention humaine :

Dans le cadre d'une décision prise de manière automatisée, sans la possibilité pour la personne concernée de s'y opposer, l'article 22(3)

du RGPD stipule que la personne concernée est en droit « d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision ». Dans une perspective similaire, mais avec une formulation un peu différente, l'article 18(4) du Décret-loi prévoit que « le responsable de traitement doit garantir une intervention humaine pour réexaminer les décisions automatisées, si la personne concernée en fait la demande ». Ce droit vise à offrir à la personne concernée une sorte de recours contre les décisions automatisées tout en lui permettant de garder un œil et d'influencer de manière significative les processus décisionnels automatisés qui l'affectent. Cependant, aucun des deux textes ne définit la nature ou l'étendue de l'intervention humaine. Les lignes directrices du G29 Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage n'apportent que peu de lumière sur ce sujet. Elles se limitent à préciser l'importance de l'intervention humaine comme élément clé, et à définir les conditions minimales pour sa mise en place (G29, 2017, p. 30). Lorsqu'une personne concernée sollicite cette intervention, l'examen de la décision doit être effectué par une personne disposant de l'autorité et la compétence nécessaires pour la révision de la décision. Cette dernière est tenue d'évaluer toutes les données pertinentes, y compris toute information supplémentaire fournie par la personne concernée.

Il est important ici de noter que ni le RGPD ni le Décret-loi fédéral n°45 ne stipulent que le droit à une intervention humaine implique nécessairement que la décision initiale soit reconsidérée. Par conséquent, les conséquences concrètes d'une contestation restent floues. De plus, même si une opportunité de reconsidération est accordée, la nature de la nouvelle décision n'est pas spécifiée. Devrait-elle être automatisée ou manuelle ?

Aucune exigence n'est formulée à cet égard (Castets-Renard, 2018).

Aussi, il convient de souligner un aspect important, mis en lumière par de nombreux auteurs, à savoir le « biais d'automatisation ». Comme nous l'avons vu dans les lignes qui précèdent, et conformément à ce que préconise le G29 dans ses lignes directives, l'intervention humaine doit être effectuée par une personne disposant de l'autorité et la compétence nécessaires pour la révision de la décision. Or, cette exigence pourrait se heurter à l'obstacle du biais d'automatisation. Ce phénomène psychologique conduit les individus à accorder une confiance excessive aux décisions de la machine, les jugeant plus fiables que leur propre discernement. Cette tendance à surestimer les capacités des systèmes automatisés risque de compromettre l'effet escompté de l'intervention humaine, dans la mesure où les personnes chargées de la révision pourraient se sentir incapables de remettre en question ou d'améliorer les décisions prises par la machine, malgré leur compétence et leur autorité.

3. Le droit à l'information :

Dans un souci de transparence des systèmes de décisions automatisées, le RGPD et le Décret-loi fédéral n°45 instaurent un droit à l'information au bénéfice de toute personne affectée par de telles décisions. Selon l'article 13, paragraphe 2, point f) et l'article 14, paragraphe 2, point g), qui traitent respectivement du droit à l'information lorsque des données à caractère personnel sont collectées directement auprès de la personne concernée et lorsque ces données ne le sont pas, le responsable du traitement doit fournir à la personne concernée des informations sur « l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la

logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée». De plus, le droit d'accès prévu par l'article 15 renforce cette transparence en accordant à la personne concernée le droit d'obtenir la confirmation de l'existence d'une prise de décision automatisée, y compris « des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ».

De son côté, le Décret-loi fédéral n°45 précise dans son article 13, paragraphe 1, point h) que la personne concernée a le droit de demander au responsable du traitement de lui fournir, sans frais, des informations sur les « décisions prises sur la base d'un traitement automatisé, y compris le profilage ».

La comparaison approfondie entre le RGPD et le Décret-loi n° 45 révèle des divergences significatives dans leur manière d'aborder le droit à l'information dans le contexte des décisions automatisées. Le RGPD, plus précis, exige une information minimale incluant, outre la mention de l'existence d'une décision automatisée, la logique sous-jacente au processus décisionnel ainsi que son importance et ses conséquences pour la personne concernée. En revanche, l'article 13, paragraphe 1, point c) du Décret-loi n° 45 présente une formulation nettement plus succincte et imprécise. Il se limite à prévoir le droit pour la personne concernée de demander des informations sur les décisions automatisées, sans fournir de directives concrètes sur la nature ou l'étendue des renseignements pouvant être demandés. Cette lacune dans la formulation du droit à l'information ouvre la voie à une information incomplète ou inadéquate, limitant ainsi l'efficacité de la protection dont devrait en bénéficier les personnes affectées par les décisions automatisées.

Une autre divergence notable entre le RGPD et le Décret-loi n° 45 réside dans le moment où les informations doivent être fournies à la personne concernée. En effet, selon le RGPD, la personne concernée dispose d'un droit d'information ex ante au titre des articles 13 et 14, ce qui signifie que la personne concernée est en droit d'être informée avant même que ses données ne soient collectées. En outre, elle bénéficie également d'un droit à l'information ex post au titre de l'article 15, c'est-à-dire après qu'une décision automatisée a été prise, lui permettant d'accéder, notamment, aux informations relatives à la logique sous-jacente du traitement automatisé, ainsi qu'à l'importance et les conséquences prévues de ce traitement. En revanche, le Décret-loi n° 45 semble adopter une approche plus restrictive en matière de transparence et d'accès à l'information que le GDPR.

Plus particulièrement, l'article 13 (c) du décret-loi n° 45 limite le droit à l'information dont dispose la personne concernée en le rendant réactif plutôt que proactif, dans la mesure où il ne s'applique qu'après que le traitement automatisé ait déjà eu lieu et uniquement sur demande. Une telle approche restrictive pourrait avoir des conséquences pratiques importantes pour la personne concernée. En effet, en rendant l'accès à l'information réactif, la personne concernée pourrait ne pas avoir connaissance que ses données sont collectées et traitées, car elle ne reçoit pas automatiquement d'informations à ce sujet. Cela signifie qu'elle pourrait ignorer l'existence même des traitements automatisés, ce qui limite sa capacité à demander des informations concernant ces traitements. De plus, le droit à l'information tel que décrit par l'article 13 (c) du décret-loi n° 45 pourrait décourager la personne concernée à demander des informations, soit par manque de sensibilisation, soit en raison de la complexité ou de la lourdeur des démarches nécessaires pour avoir accès aux informations.

4. Un droit à l'explication

Le droit à l'explication des décisions automatisées constitue un autre point de divergence entre les deux textes étudiés. Ainsi, contrairement au décret-loi n° 45, dont l'article 13 se contentait de prévoir le droit de s'informer de l'existence de telles décisions, le RGPD se révèle nettement plus exigeant en matière de transparence.

En effet, au sujet du RGPD, parmi les questions relatives aux décisions automatisées, le droit à l'explication constitue un aspect théorique majeur. Ce concept a fait l'objet d'intenses discussions doctrinales, notamment en raison de ses implications profondes pour la transparence des décisions algorithmiques et la protection des droits des personnes concernées par ces décisions. Ces discussions portaient sur la question de savoir si les individus faisant l'objet d'une décision automatisée disposent d'un droit opposable d'obtenir des explications sur la logique impliquée dans les processus de décision algorithmique qui les affectent de manière significative (Kaminski, 2019). La réponse à cette question est cruciale pour comprendre les implications pratiques de ce droit. L'inclusion d'un droit à l'explication signifierait que la personne concernée aurait non seulement la possibilité de communiquer avec un humain (par opposition à une machine), mais également de comprendre les critères et les fondements de la décision automatisée prise à son égard. Cela pourrait impliquer la révélation des données prises en compte, des algorithmes utilisés, et des logiques sous-jacentes au processus décisionnel.

Bien que le RGPD ne codifie pas explicitement un «droit à l'explication», certains auteurs estiment que le RGPD ne prévoit qu'un «droit d'être informé» de l'existence d'une prise de décision automatisée, plutôt qu'un droit complet à l'explication des décisions spécifiques (Wachter et al., 2017 ; Castets-Renard, 2018). À l'inverse, d'autres soutiennent qu'un droit à l'explication des décisions automatisées découle implicitement de la lecture combinée de l'article 22 du RGPD, des articles 13 et 15, qui traitent respectivement du droit à l'information et au droit d'accès, ainsi que du considérant 71 du RGPD (Goodman & Flaxman, 2017)(1). Par ailleurs, un véritable droit à l'explication peut être déduit d'une interprétation systématique du RGPD, surtout lorsqu'on prend en compte ses principes fondamentaux de transparence et de responsabilité (Selbst & Powles, 2018). Cette interprétation est d'autant plus pertinente qu'elle s'aligne avec l'esprit général du règlement visant à donner aux individus un contrôle effectif sur leurs données personnelles. Toutefois, la mise en œuvre pratique de ce droit pourrait se heurter en pratique à des obstacles significatifs, notamment dans certains cas de décisions automatisées basées sur des algorithmes complexes où la fourniture d'une explication claire et compréhensible peut s'avérer techniquement difficile, voire impossible (Castets-Renard, 2018).

B. Les obligations du responsable du traitement

En plus des droits des utilisateurs détaillés précédemment, le RGPD et le Décret-loi n° 45 imposent également des exigences spécifiques concernant

- (1) Selon le considérant 71 du RGPD, la prise de décision automatisée *« devrait être assorti de garanties appropriées, qui devraient comprendre une information spécifique de la personne concernée ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision »*.

le processus et la conception des systèmes de prise de décision automatisée (ADM). Ces exigences incluent notamment la protection des données dès la conception, connue sous le nom de «Privacy by Design» (1), ainsi que l'analyse d'impact relative à la protection des données (2).

1. La protection des données dès la conception

La protection des données dès la conception met l'accent sur l'intégration proactive des mesures de protection des données dès les premières étapes du développement d'un produit ou d'un service, plutôt que de les ajouter comme une couche supplémentaire après coup (Cavoukian, 2009).

Le RGPD ainsi que le Décret-loi n° 45 imposent des exigences spécifiques concernant la conception technique des systèmes de traitement des données. Plus précisément, l'Article 25 (1) du RGPD dispose que « le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée ». Cette approche est également reflétée dans l'article 8(2) du Décret-loi n° 45 qui stipule que le responsable du traitement doit « appliquer les procédures et mesures techniques et organisationnelles appropriées pour protéger les Données Personnelles dès la phase de conception, que ce soit lors de l'identification des moyens de traitement ou pendant le traitement, en tenant compte du coût de mise en œuvre de ces procédures ainsi que de la nature, de la portée et des finalités du traitement ».

Le principe de la protection des données dès la conception est particulièrement pertinent dans le contexte de la prise de décision automatisée, où l'opacité des algorithmes peut entraîner des conséquences imprévues, telles que la discrimination et les violations des droits individuels (Bu et al., 2020). En intégrant la protection de la vie privée dès la conception, les développeurs peuvent anticiper et atténuer ces risques potentiels. Cela signifie qu'ils doivent prendre en compte les implications sur la vie privée dès les premières étapes du développement d'un système ou d'un produit. Une évaluation rigoureuse des impacts sur la vie privée est essentielle pour identifier les points faibles potentiels où des violations pourraient se produire. En outre, il est nécessaire d'instaurer des mesures de protection robustes, notamment le chiffrement, l'anonymisation et des contrôles d'accès stricts, afin de garantir que les systèmes respectent à la fois les normes juridiques et les principes éthiques.

Néanmoins, le principe de la protection des données personnelles dès la conception fait face à des défis significatifs dans sa mise en œuvre effective (Kroener & Wright, 2014 ; Dray & Benaissa). Le défi principal réside dans la nature pratique de son application, particulièrement en ce qui concerne l'évaluation des risques. Les responsables du traitement des données se trouvent souvent confrontés à un manque d'informations concrètes pour mettre en place des mesures de protection efficaces (Spiekermann, 2012).

L'aspect ouvert et évolutif de l'évaluation des risques constitue un obstacle majeur. En effet, les menaces à la protection des données sont en constante évolution, et il est difficile de prévoir tous les scénarios possibles (Alhazmi & Arachchilage, 2020). Cette réalité contraint les responsables du traitement à opérer avec des données partielles ou approximatives, pouvant ainsi affecter l'efficacité des dispositifs de protection instaurés.

Cette incertitude est amplifiée par la complexité croissante des systèmes technologiques et des flux de données. Les responsables du traitement doivent non seulement comprendre les risques actuels, mais aussi anticiper les menaces futures potentielles. Cette tâche devient particulièrement ardue dans un environnement technologique qui évolue rapidement et où de nouvelles vulnérabilités peuvent apparaître à tout moment (Gürses et al., 2011).

Par ailleurs, un autre défi majeur dans l'implémentation du principe de protection des données dès la conception réside dans la difficulté d'équilibrer les différents aspects de la protection des données personnelles. En effet, la protection des données englobe un large éventail de droits relatifs aux données, et ces droits peuvent entrer en conflit les uns avec les autres. Ainsi, par exemple, la protection des données dans le cadre de la prise de décision automatisée implique requiert la minimisation de la quantité de données personnelles stockées et traitées, alors que pour contester de manière appropriée une décision automatisée pourrait nécessiter davantage d'informations que celles strictement requises à des fins décisionnelles (Veale et al., 2018).

Enfin, le manque de standards précis et uniformisés pour l'évaluation des risques complique davantage la situation (Colesky et al., 2016). Les entreprises peuvent avoir des interprétations divergentes des risques et des mesures techniques nécessaires, ce qui pourrait conduire à une protection inégale des données personnelles selon les entreprises et les secteurs d'activité.

2. L'analyse d'impact relative à la protection des données

L'obligation de réaliser une Analyse d'Impact relative à la Protection des Données (AIPD) représente un pilier essentiel de la protection préventive des données personnelles, particulièrement dans le contexte du traitement automatisé des données personnelles. Cette obligation agit comme un mécanisme de précaution qui permet d'identifier et d'évaluer en amont les risques potentiels liés au processus décisionnel automatisé, ce qui est en parfaite adéquation avec le principe protection des données dès la conception détaillée plus haut. Elle contraint les responsables du traitement à adopter une approche proactive plutôt que réactive en matière de protection des données, en les obligeant à examiner minutieusement les impacts possibles de leurs activités de traitement envisagées avant leur mise en œuvre (Raimondo,2023).

Selon l'article 35 du RGPD et l'article 21 du Décret-loi n° 45, cette obligation s'impose particulièrement lorsqu'un traitement systématique et automatisé des aspects personnels concernant des personnes physiques est mis en œuvre. L'objectif est de s'assurer de la conformité du processus de décision aux exigences règlementaires en matière de protection des données. L'AIPD doit être réalisée en amont du traitement et doit comprendre, au minimum, une description systématique des opérations de traitement envisagées, une évaluation de leur nécessité et de leur proportionnalité, ainsi qu'une analyse des risques pour les droits et libertés des personnes concernées (Raimondo, 2023). Les responsables du traitement doivent également documenter les mesures prévues pour faire face à ces risques, notamment les garanties, mesures de sécurité et mécanismes visant à assurer la protection des données personnelles.

Par ailleurs, le RGPD et le Décret-loi n° 45 prévoient également une approche itérative. En effet, aux termes de l'Article 35(11) RGPD et de l'Article 21(7) du Décret-loi, lorsque le niveau de risque lié au système change, l'entreprise doit vérifier sa conformité avec sa propre analyse d'impact et potentiellement réviser l'analyse d'impact initial.

Dans ses Lignes directrices relatives aux AIPD, le G29 va plus loin en suggérant, à titre de bonne pratique, que les AIPD devraient faire l'objet d'un examen continu et être régulièrement réévaluées (G29, 2017). Ainsi, « la réalisation d'une AIPD relève d'un processus continu et n'est pas un exercice ponctuel », en particulier « lorsque l'opération de traitement est dynamique et soumise à de constants changements » (G29, 2017, p. 17). Conformément aux articles 35 (7) du RGPD et 21 (3) du Décret-loi n° 45, ce processus continu implique l'évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités, le déploiement de mesures envisagées pour faire face aux risques, la documentation de leur efficacité par le biais d'un suivi, et la réintégration de ces informations dans l'évaluation des risques.

Conclusion :

En conclusion, notre analyse comparative du RGPD européen et du Décret-loi émirati n°45 de 2021 révèle une dynamique juridique complexe dans la régulation des décisions automatisées, illustrant les défis contemporains de la protection des données personnelles.

Si les deux cadres réglementaires partagent certains principes fondamentaux, l'approche européenne, plus mature et exhaustive, offre un modèle particulièrement pertinent pour l'évolution future de la législation émiratie. Le RGPD, largement reconnu comme l'un des cadres les plus

rigoureux au monde en matière de protection des données, propose des mécanismes éprouvés de protection des droits individuels et de régulation algorithmique. Il serait opportun pour le législateur Emirati d'envisager de les intégrer dans son arsenal juridique.

Nous recommandons ainsi que la législation émiratie s'aligne davantage sur les standards européens, notamment en ce qui concerne la transparence des processus de décision automatisés. Cette harmonisation aurait le double avantage de renforcer la protection des données personnelles aux Émirats Arabes Unis tout en facilitant les échanges de données avec l'Union européenne, un partenaire économique majeur.

À l'heure où l'intelligence artificielle redéfinit les contours de la prise de décision, l'adoption des meilleures pratiques européennes permettrait aux Émirats Arabes Unis de se positionner comme un leader régional en matière de protection des données, tout en préservant leurs spécificités culturelles et économiques. Cette évolution apparaît comme une étape cruciale pour faire face aux défis futurs posés par l'utilisation croissante des outils décisionnels automatisés.

References

- AlgorithmWatch. (2019). Automating society, Available at: <https://algorithmwatch.org/en/automating-society-2019/>, accessed on 11 November 2024.
- Alhazmi, A., & Arachchilage, N. A. G. (2020). Why are developers struggling to put GDPR into practice when developing Privacy-Preserving software systems. arXiv preprint arXiv:2008.02987.
- Artzt, M., & Dung, T. V. (2022). Artificial intelligence and data protection: How to reconcile both areas from the European law perspective. *Vietnamese Journal of Legal Sciences*, 7(2), 39-58. <https://doi.org/10.2478/vjls-2022-0007>. <https://doi.org/10.2478/vjls-2022-0007>
- Ben Yacoub H.. Du réel au virtuel, l'art de poser les bonnes questions
- Bensamoun, A., & Loiseau, G. (2017). L'intégration de l'intelligence artificielle dans l'ordre juridique en droit commun: questions de temps. *Daloz IP/IT: droit de la propriété intellectuelle et du numérique*, (04), 239-243.
- Besse, P., Castets-Renard, C., Garivier, A., & Loubes, J. M. (2018). L'IA du quotidien peut-elle être éthique?. *Statistique et Société*, 6(3), 9-31. <https://doi.org/10.3406/staso.2018.1083>
- Bhutta, N., Hizmo, A., & Ringo, D. (2022). How much does racial bias affect mortgage lending? Evidence from human and algorithmic credit decisions, accessible sur: <https://www.federalreserve.gov/econres/feds/files/2022067pap.pdf>. <https://doi.org/10.2139/ssrn.3887663>
- Borch, C. (2016). High-frequency trading, algorithmic finance and the Flash Crash: reflections on eventalization. *Economy and Society*, 45(3-4), 350-378. <https://doi.org/10.1080/03085147.2016.1263034>
- Brkan, M., & Bonnet, G. (2020). Legal and technical feasibility of the GDPR's quest for explanation of algorithmic decisions: of black boxes, white boxes and fata morganas. *European Journal of Risk Regulation*, 11(1), 18-50. <https://doi.org/10.1017/err.2020.10>
- Bu, F., Wang, N., Jiang, B., & Liang, H. (2020). "Privacy by Design" implementation: Information system engineers' perspective. *International Journal of Information Management*, 53, 102124. <https://doi.org/10.1016/j.ijinfomgt.2020.102124>
- Castets-Renard, C. (2016). Brève analyse du règlement général relatif à la protection des données personnelles. *Daloz IP/IT : droit de la propriété intellectuelle et du numérique*, (07 et 08), 331.
- Castets-Renard, C. (2018). Régulation des algorithmes et gouvernance du machine learning : vers une transparence et « explicabilité » des décisions algorithmiques ?. *Revue Droit & Affaires, Revue Paris II Assas*, 15ème édition.
- Castets-Renard, C. (2019). Accountability of algorithms in the GDPR and beyond: a European legal framework on automated decision-making. *Fordham Intell. Prop.*

- Media & Ent. LJ, 30, 91. <https://doi.org/10.2139/ssrn.3391266>
- Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada, 5, 12.
- Chemlali, L., Salmi, A., & Benseddik, L. (2023). A reflection on the UAE's new data protection law: A comparative approach with GDPR. *Journal of Data Protection & Privacy*, 6(1), 24-36. <https://doi.org/10.69554/OPEG2767>
- Christodoulou, P., & Limniotis, K. (2024). Data Protection Issues in Automated Decision-Making Systems Based on Machine Learning: Research Challenges. *Network*, 4(1), 91-113. <https://doi.org/10.3390/network4010005>
- Citron, D. K. (2007). Technological due process. *Wash. UL Rev.*, 85, 1249.
- Colesky, M., Hoepman, J. H., & Hillen, C. (2016, May). A critical analysis of privacy design strategies. In 2016 IEEE security and privacy workshops (SPW) (pp. 33-40). IEEE. <https://doi.org/10.1109/SPW.2016.23>
- Comité Européen sur la Protection des Données (CEPD), Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679, version 1.1, Adoptées le 4 mai 2020, disponible sur : https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_fr.pdf.
- Dary, M., & Benaissa, L. (2016). Privacy by Design: un principe de protection séduisant mais complexe à mettre en œuvre. *Daloz IP/IT*, 2016(10).
- Décret-loi fédéral n° 45/2021 relatif à la protection des données à caractère personnel (2021). *Gazette officielle*, 712, 15
- Deltorn, J. M. (2017). La protection des données personnelles face aux algorithmes prédictifs. *Revue des droits et libertés fondamentaux*, 1-18.
- Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. *Duke L. & Tech. Rev.*, 16, 18. <https://doi.org/10.31228/osf.io/97upg>
- Explainable AI: the basics, (The Royal Society: London, 2019), https://ec.europa.eu/futurium/en/system/files/ged/ai-and-interpretability-policy-briefing_creative_commons.pdf.
- Fischer, J. E., Greenhalgh, C., Jiang, W., Ramchurn, S. D., Wu, F., & Rodden, T. (2021). In the loop or on the loop? Interactional arrangements to support team coordination with a planning agent. *Concurrency and Computation: Practice and Experience*, 33(8), e4082. <https://doi.org/10.1002/cpe.4082>
- Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a "right to explanation". *AI magazine*, 38(3), 50-57. <https://doi.org/10.1609/aimag.v38i3.2741>
- Grant, D.G., Behrends, J. & Basl, J. What we owe to decision-subjects: beyond transparency and explanation in automated decision-making. *Philos Stud* (2023). <https://doi.org/10.1007/s11099-023-01450-0>

- org/10.1007/s11098-023-02013-6. <https://doi.org/10.1007/s11098-023-02013-6>
- Groupe de travail « Article 29 » sur la protection des données. (2017). 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. WP 248 rév.01.
- Groupe de travail « Article 29 » sur la protection des données. (2017). Avis 2/2017 sur le traitement des données sur le lieu de travail, disponible sur : <https://ec.europa.eu/newsroom/article29/items/610169/en>.
- Gürses, S., Troncoso, C., & Diaz, C. (2011). Engineering privacy by design. *Computers, Privacy & Data Protection*, 14(3), 25.
- Hurley, M., & Adebayo, J. (2016). Credit scoring in the era of big data. *Yale JL & Tech.*, 18, 148.
- Ivanov, S. H. (2023). Automated decision-making. *foresight*, 25(1), 4-19. <https://doi.org/10.1108/FS-09-2021-0183>
- Kaminski, M. E. Binary Governance: Lessons from the GDPR's approach to Algorithmic Accountability' (2019). *Southern California Law Review*, 92, 1529. <https://doi.org/10.2139/ssrn.3351404>
- Kaminski, M. E. The right to explanation, explained (2019). *Berkeley Technology Law Journal*, 34(1), 189-215. <https://doi.org/10.15779/Z38TD9N83H>
- Kaminski, M. E., & Urban, J. M. (2021). The right to contest AI. *Columbia Law Review*, 121(7), 1957-2048.
- Kroener, I., & Wright, D. (2014). A strategy for operationalizing privacy by design. *The Information Society*, 30(5), 355-365. <https://doi.org/10.1080/01972243.2014.944730>
- Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, version révisée du 6 février 2018, WP251 rev.01, Accessible sur : <https://ec.europa.eu/newsroom/article29/items/612053>.
- Lukács, A., & Váradi, S. (2023). GDPR-compliant AI-based automated decision-making in the world of work. *Computer Law & Security Review*, 50, 105848. <https://doi.org/10.1016/j.clsr.2023.105848>
- Markus, Aniek F., Jan A. Kors, and Peter R. Rijnbeek. "The role of explainability in creating trustworthy artificial intelligence for health care: a comprehensive survey of the terminology, design choices, and evaluation strategies." *Journal of biomedical informatics* 113 (2021) : 103655. <https://doi.org/10.1016/j.jbi.2020.103655>
- Mendoza, I., & Bygrave, L. A. (2017). The right not to be subject to automated decisions based on profiling. *EU internet law: Regulation and enforcement*, 77-98. https://doi.org/10.1007/978-3-319-64955-9_4
- Parlement européen et Conseil de l'Union européenne. (2016). Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection

- des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données). Journal officiel de l'Union européenne, L 119, 1-88. <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679>.
- Prince, A. E., & Schwarcz, D. (2019). Proxy discrimination in the age of artificial intelligence and big data. *Iowa L. Rev.*, 105, 1257.
- Rahwan, I., Cebrian, M., Obradovich, N., Bongard, J., Bonnefon, J. F., Breazeal, C., ... & Wellman, M. (2019). Machine behaviour. *Nature*, 568(7753), 477-486. <https://doi.org/10.1038/s41586-019-1138-y>
- Raimondo, L. (2021). *La protection des données personnelles en 100 Questions/Réponses*. Editions Ellipses.
- Selbst, A., & Powles, J. (2018, January). "Meaningful information" and the right to explanation. In conference on fairness, accountability and transparency (pp. 48-48). PMLR.
- Selbst, Andrew D., and Solon Barocas. "The intuitive appeal of explainable machines." *Fordham L. Rev.* 87 (2018): 1085. <https://doi.org/10.2139/ssrn.3126971>
- Spann, M., Bertini, M., Koenigsberg, O., Zeithammer, R., Aparicio, D., Chen, Y., ... & Yoo, H. (2024). Algorithmic Pricing: Implications for Consumers, Managers, and Regulators (No. w32540). National Bureau of Economic Research. <https://doi.org/10.2139/ssrn.4859392>
- Spiekermann, S. (2012). The challenges of privacy by design. *Communications of the ACM*, 55(7), 38-40. <https://doi.org/10.1145/2209249.2209263>
- Thouvenin, F., Fruh, A., & Henseler, S. (2022). Article 22 GDPR on Automated Individual Decision-Making: Prohibition or Data Subject Right?. *Eur. Data Prot. L. Rev.*, 8, 183. <https://doi.org/10.21552/edpl/2022/2/6>
- Tosoni, L. (2021). The right to object to automated individual decisions: resolving the ambiguity of Article 22 (1) of the General Data Protection Regulation. *International Data Privacy Law*, 11(2), 145-162. <https://doi.org/10.1093/idpl/ipaa024>
- Veale, M., Binns, R., & Ausloos, J. (2018). When data protection by design and data subject rights clash. *International Data Privacy Law*, 8(2), 105-123. <https://doi.org/10.1093/idpl/ipy002>
- Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International data privacy law*, 7(2), 76-99. <https://doi.org/10.1093/idpl/ix005>
- Wiedemann, K. (2018). Automated processing of personal data for the evaluation of personality traits: Legal and ethical issues. *Max Planck Institute for Innovation & Competition Research Paper*, (18-04). <https://doi.org/10.2139/ssrn.3102933>

Automated Decision-Making

A Comparative Analysis between the European GDPR and the Emirati Federal Decree-Law No. 45 of 2021

Laroussi Chemlali⁽¹⁾

Received on: 21-11-2024

Accepted on: 16-01-2025

Abstract:

In the digital age, the increasing use of automated decision-making systems by businesses and public institutions raises major challenges regarding personal data protection and fundamental rights. This study offers a comparative analysis of the legal framework governing automated decision-making between the European General Data Protection Regulation (GDPR) and the UAE Federal Decree-Law No. 45 of 2021 regarding personal data protection, highlighting the different approaches adopted by these two texts to regulate the use of automated decision-making systems. This research examines in depth the convergences and divergences between these two regulatory frameworks, particularly regarding the guarantees offered to data subjects and the obligations imposed on data controllers in this context. To achieve this, we began by defining the contours of the concept of automated decision-making and the challenges it poses, before studying the guarantees and obligations provided by the European GDPR and UAE Decree-Law No. 45.

Keywords: Automated decision-making, data protection, GDPR, Federal Decree-Law No. 45/2021.

(1) College of Law - Ajman University (Ajman - United Arab Emirates)

اتخاذ القرارات الآلي ”دراسة مقارنة بين اللائحة العامة لحماية البيانات الأوروبية والمرسوم بقانون اتحادي إماراتي رقم 45 لسنة 2021“

لعروسي شملاي⁽¹⁾

ملخص البحث:

في العصر الرقمي، يُثير تزايد استخدام أنظمة اتخاذ القرارات الآلية من قبل الشركات والمؤسسات العامة تحديات كبيرة فيما يتعلق بحماية البيانات الشخصية والحقوق الأساسية. تُقدم هذه الدراسة تحليلاً مقارناً للإطار القانوني الذي يُنظم اتخاذ القرارات الآلية بين اللائحة العامة لحماية البيانات الأوروبية (GDPR) والرسوم بقانون اتحادي إماراتي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية، مُسلطاً الضوء على الاختلافات في النهج التي يتبناها هذان النصان لتنظيم استخدام أنظمة اتخاذ القرارات الآلية. يتناول البحث بالتفصيل أوجه التقارب والاختلاف بين هذين الإطارين التنظيميين، لا سيما فيما يتعلق بالضمانات المُقدمة للأفراد المعنيين بالبيانات والالتزامات المفروضة على مُتحكمي البيانات في هذا السياق. لتحقيق ذلك، بدأنا بتحديد معالم مفهوم اتخاذ القرارات الآلي والتحديات التي يطرحها، قبل دراسة الضمانات والالتزامات التي يوفرها النظام الأوروبي العام لحماية البيانات (GDPR) والرسوم بقانون رقم 45 الصادر عن دولة الإمارات العربية المتحدة

الكلمات الدالة: اتخاذ القرارات الآلي، حماية البيانات، النظام الأوروبي العام لحماية البيانات (GDPR)، المرسوم بقانون رقم 45 لسنة 2021.

(1) كلية الحقوق - جامعة عجمان (عجمان - الإمارات العربية المتحدة)