Guide pratique du respect des valeurs de l'Union européenne et systèmes d'intelligence artificielle

Baptiste Martinez, Marion Ho-Dac

Guide pratique : Respect des valeurs de l'Union européenne et systèmes d'intelligence artificielle

METHODOLOGIE ET DOCUMENTS PRATIQUES DU RESPECT DES VALEURS DE L'UNION EUROPEENNE PAR LES SYSTEMES D'INTELLIGENCE ARTIFICIELLE DES LA CONCEPTION ET TOUT AU LONG DU CYCLE DE VIE

Baptiste Martinez, Ingénieur de recherche & Marion Ho-Dac, Professeure de droit privé

UNIVERSITE D'ARTOIS, CENTRE DROIT ETHIQUE ET PROCEDURES UR2471

Résumé : Les valeurs de l'Union européenne (VUE) sont les valeurs fondamentales – (notamment) de respect de la dignité humaine, de liberté, de démocratie, d'égalité, de l'État de droit, ainsi que de respect des droits de l'homme (art. 2 TUE) – autour desquelles s'est construite l'Union et qui rassemblent les différentes sociétés européennes. Leur respect est au cœur de la règlementation des systèmes d'intelligence artificielle (SIA) élaborée par l'Union (AI Act). L'AI Act a en effet pour objectif « *d'améliorer le fonctionnement du marché intérieur en établissant un cadre juridique uniforme, en particulier pour le développement, la mise sur le marché, la mise en service et l'utilisation de systèmes d'intelligence artificielle […] dans le respect des valeurs de l'Union […]* » (AI Act, cons. 1er).
Le respect des VUE est ainsi un élément essentiel à prendre en compte pour la conception et le développement des SIA par les fournisseurs et lors leur utilisation par les déployeurs. D'un point de vue méthodologique, la conformité aux VUE pourrait prendre appui sur une étude d'impact du SIA sur les VUE afin, d'une part, d'identifier les risques que le SIA présente pour les VUE et, d'autre part, de définir les mesures de gestion des risques permettant d'atteindre un niveau de risque acceptable, et ce dès la conception du SIA.
A cette fin, ce *Guide pratique du respect des VUE* est proposé aux industriels et aux parties prenantes de l'écosystème de l'IA. Il comporte trois parties : une cartographie présentant certaines VUE et leurs droits et principes fondamentaux de concrétisation ; la méthodologie de l'étude d'impact sur les VUE à appliquer aux SIA, et sa mise en œuvre ; et enfin, en annexe, les documents pratiques permettant de procéder à l'étude d'impact, complétés par d'autres ressources documentaires.

Abstract: The values of the European Union (VEU) are the fundamental values – (in particular) of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights (art. 2 TEU) – around which the Union was built and which unite the various European societies. Respect for these principles is at the heart of the EU regulation of artificial intelligence systems (AI Act). The objective of the AI Act is "*to improve the functioning of the internal market by establishing a uniform legal framework, in particular for the development, placing on the market, putting into service and use of artificial intelligence systems [...] in a manner consistent with the values of the Union [...]*" (AI Act, cons. 1).
Compliance with the VEU is therefore an essential element to be taken into account in the design and development of AI systems (AIS) by suppliers and in their use by deployers. From a methodological point of view, compliance with the VEU could be based on an impact assessment of the AIS on the VUE in order, on the one hand, to identify the risks that the AIS presents for the VUE and, on the other hand, to define the risk management measures making it possible to achieve an acceptable level of risk, including by design.
To this end, this *Practical Guide to VEU Compliance* is offered to manufacturers and stakeholders in the AI ecosystem. It is divided into three parts: a map presenting certain VEU and their attached fundamental rights and principles; the methodology for the impact assessment on the VEU to be applied to AIS, and its implementation; and finally, in the appendix, practical documents for carrying out the impact assessment, supplemented by other documentary resources.

Ce travail a été soutenu par le gouvernement français dans le cadre du programme « France 2030 », au sein de l'Institut de Recherche Technologique SystemX dans le cadre du projet Confiance.ai.

Sommaire :

I. Présentation du Guide pratique

A. Pourquoi un Guide pratique ?

1. Les valeurs de l'UE (VUE)

1. Les valeurs de l'Union européenne : présentation. Les valeurs de l'Union européenne (VUE) sont les valeurs fondamentales autour desquelles s'est construite l'Union et qui rassemblent les différentes sociétés européennes.

Ces valeurs sont présentées par l'article 2 du Traité sur l'Union européenne (TUE) :

> *« L'Union est fondée sur les valeurs de respect de la dignité humaine, de liberté, de démocratie, d'égalité, de l'État de droit, ainsi que de respect des droits de l'homme, y compris des droits des personnes appartenant à des minorités. Ces valeurs sont communes aux États membres dans une société caractérisée par le pluralisme, la non-discrimination, la tolérance, la justice, la solidarité et l'égalité entre les femmes et les hommes ».*

2. Les VUE et le règlement européen sur l'intelligence artificielle (AI Act). Le respect des valeurs de l'Union européenne (VUE) est au cœur de la règlementation des systèmes d'intelligence artificielle élaborée par l'Union européenne (AI Act, règl. UE 2024/1689 du 13 juin 2024).

L'AI Act a pour objectif « d'améliorer le fonctionnement du marché intérieur en établissant un cadre juridique uniforme, en particulier pour le développement, la mise sur le marché, la mise en service et l'utilisation de systèmes d'intelligence artificielle […] dans le respect des valeurs de l'Union […] » (AI Act, cons. 1er). Le respect des VUE apparaît ainsi comme un élément fondamental de l'encadrement juridique des systèmes d'intelligence artificielle (SIA) dans le marché européen. L'ancrage de la législation de l'Union en matière de SIA dans les VUE ressort également du considérant 6 de l'AI Act, indiquant que « l'IA et son cadre réglementaire doivent impérativement être élaborés dans le respect des valeurs de l'Union consacrées à l'article 2 du traité sur l'Union européenne ».

2. Le respect des VUE par les systèmes d'intelligence artificielle (SIA)

3. Les enjeux du respect des VUE : la mise sur le marché ou la mise en service du SIA. Le respect des VUE n'est pas qu'un discours politique attaché à la règlementation sur l'IA. Il s'agit bien plus d'une dynamique substantielle emportant des répercussions pratiques concrètes et importantes.

En effet, d'une part, certaines pratiques sont expressément considérées comme interdites par l'AI Act car « elles sont contraires aux valeurs de l'Union relatives au respect de la dignité humaine, à la liberté, à l'égalité, à la démocratie et à l'état de droit, ainsi qu'aux droits fondamentaux consacrés dans la Charte, y compris le droit à la non-discrimination, le droit à la protection des données et à la vie privée et les droits de l'enfant » (AI Act, cons. 28).

Il s'agit des pratiques présentées par l'article 5 de l'AI Act. La mise en œuvre de ces pratiques est interdite et il n'est pas possible de commercialiser ou de mettre en service, en principe, des SIA recourant à ces pratiques.

D'autre part, dans la mesure où l'AI Act s'inscrit dans le respect des VUE et qu'il vise à garantir la création de SIA « conformes aux valeurs de l'Union » (AI Act, cons. 6 et 8), tout SIA dont l'utilisation porterait atteinte aux VUE, même sans mettre en œuvre une des pratiques prohibées de l'article 5, devrait être considéré comme interdit, empêchant ainsi sa commercialisation ou sa mise en service.

4. Le respect des VUE dès la conception et tout au long du cycle de vie du SIA. Il apparaît ainsi que le respect des VUE est un élément essentiel à prendre en compte pour la conception et le développement de SIA par les fournisseurs.

Pour garantir le respect des VUE, la conformité aux VUE devrait être une préoccupation des fournisseurs dès la conception des SIA. D'un point de vue méthodologique, elle devrait prendre appui sur l'étude d'impact (v. *infra*). L'absence de prise en compte des VUE dès la conception implique le risque, en premier lieu, de mettre sur le marché un SIA qui ne serait pas conforme aux VUE. Ceci pourrait avoir des conséquences juridiques et opérationnelles graves, comme un action en responsabilité formée par les victimes ou une obligation de retrait du SIA prononcée par les autorités administratives ou juridictionnelles. En second lieu, la prise en compte tardive des VUE peut impliquer de reprendre le processus de production du SIA à la phase de conception alors même que le projet avait avancé, entraînant un surcoût de production.

Le respect des VUE doit également être une préoccupation tout au long du cycle de vie du SIA, de sa conception à son retrait. Ainsi, il convient de réévaluer la conformité du SIA aux VUE, même après la première mise sur le marché, à des périodes régulières et en cas de modification substantielle[1] du SIA.

3. Un Guide à destination des industriels

5. Un Guide s'adressant aux professionnels de l'IA. C'est aux fins de permettre aux professionnels de l'IA de garantir le respect des VUE dès la conception et tout au long du cycle de vie des SIA que le présent Guide a été rédigé. Les professionnels de l'IA sont désignés en tant qu'opérateurs par l'AI Act. Il s'agit des fournisseurs, des fabricants de produits, des déployeurs, des mandataires, des importateurs ou des distributeurs (AI Act, art. 3, §8).

6. Un Guide s'adressant aux fournisseurs. Ce Guide s'adresse particulièrement aux fournisseurs de SIA. Le fournisseur est défini par l'AI Act comme « une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA ou un modèle d'IA à usage général et le met sur le marché ou met le système d'IA en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit » (AI Act, art. 3, §3).

Le fournisseur est principalement concerné par ce Guide car il est le plus à même de gérer les risques pour les VUE : il maîtrise la conception du SIA et en connaît les aspects techniques. Il est compétent pour appréhender les conséquences de son SIA sur les VUE et pour identifier les mesures adaptées en vue de gérer ces risques et en particulier les risques les plus graves, dits risques systémiques. En ce sens, l'AI Act prévoit que les fournisseurs de SIA

à haut risque doivent élaborer un système de gestion des risques, le documenter et le tenir à jour (AI Act, art. 9). Ce système inclut notamment « l'identification et l'analyse des risques connus et raisonnablement prévisibles que le système d'IA à haut risque peut poser pour la santé, la sécurité ou les droits fondamentaux […] » (AI Act, art. 9, §2 sous a). En ce sens, l'analyse des risques pour les VUE pourrait aisément s'insérer dans ce schéma règlementaire.

Le Guide pratique a pour vocation d'aider les fournisseurs à produire des SIA respectueux des VUE dès la conception et tout au long du cycle de vie du SIA.

La réalisation de l'étude d'impact sur les VUE – méthodologie sur laquelle ce guide prend appui (v. *infra*) – peut également être un gage de confiance pour les déployeurs du SIA ou les personnes concernées. Les résultats de l'étude d'impact pourraient être mentionnés dans la notice d'utilisation du SIA ou servir d'indication utile pour les déployeurs devant réaliser une analyse d'impact sur les droits fondamentaux en vertu de l'article 27 de l'AI Act.

7. Un Guide s'adressant aux déployeurs. Ce Guide s'adresse également aux déployeurs. Le déployeur est selon l'AI Act « une personne physique ou morale, une autorité publique, une agence ou un autre organisme utilisant sous sa propre autorité un système d'IA sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel » (AI Act, art. 3, §4).

Les déployeurs, en tant qu'utilisateurs de SIA, ont à connaître des risques sectoriels, individuels ou collectifs associés à l'utilisation d'un SIA ; ils peuvent également être directement confrontés à des incidents survenus dans le contexte de SIA. C'est pour cette raison que l'article 27 de l'AI Act a mis à la charge de certains d'entre eux une obligation spécifique de réalisation d'une analyse d'impact sur les droits fondamentaux. Ils sont les mieux placés pour gérer ces risques dans un cas d'usage délimité et pour informer le fournisseur que ces risques existent.

Aussi, les déployeurs devraient être soucieux de s'assurer du respect des VUE notamment au regard des dispositions de l'article 25 de l'AI Act qui prévoit un système de responsabilité tout au long de la chaîne de valeur de l'IA. Selon cet article, tout distributeur, importateur, déployeur ou autre tiers peut être considéré, à certaines conditions, comme fournisseur du SIA et être soumis aux obligations incombant à ce dernier au titre de l'article 16 de l'AI Act, étant inclus le respect des VUE. Dans ces conditions, le déployeur pourrait être amené à réaliser une étude d'impact sur les VUE pour s'assurer qu'il utilise le SIA d'une façon conforme aux VUE.

B. Mode d'emploi du Guide pratique

1. La mise en œuvre du Guide pratique

8. Les différents éléments du Guide. Le Guide pratique comporte trois parties :

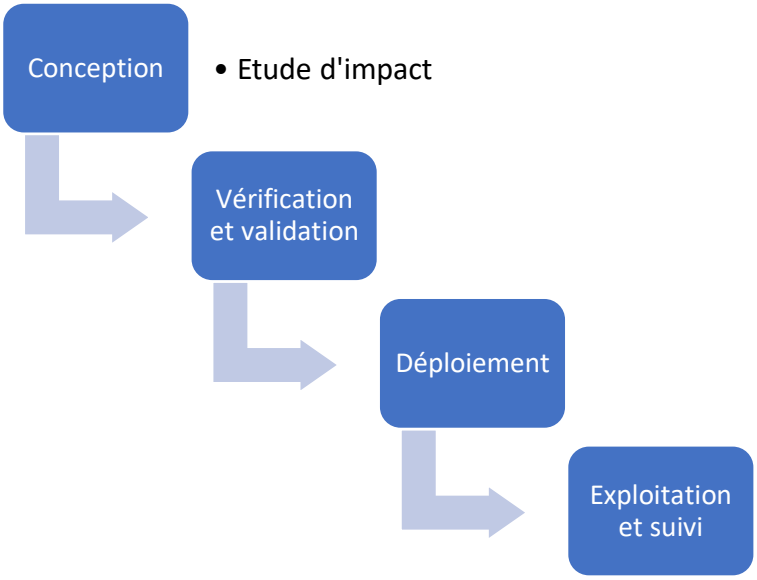
- une cartographie présentant certaines VUE et leurs droits et principes fondamentaux de concrétisation ;
- la méthodologie de l'étude d'impact sur les VUE à appliquer aux SIA, et sa mise en œuvre ;
- et enfin, en annexe, les documents pratiques permettant de procéder à l'étude d'impact, complétés par d'autres ressources documentaires.

9. La présentation de l'étude d'impact. L'élément central du Guide est l'étude d'impact. Cette étude d'impact a pour objectifs :

- d'*identifier les risques* que le SIA présente pour les VUE ;
- de définir les mesures de gestion des risques permettant d'atteindre un *niveau de risque acceptable* ;
- et ce *dès la conception* du SIA.

Identifier les risques	Atteindre un niveau de risque acceptable	Dès la conception
• Il s'agit de déterminer précisement les sources de risques pour les VUE potentiellement affectées. • Il s'agit également d'évaluer le niveau des risques.	• L'AI Act admet des risques résiduels "acceptables". • Pour atteindre un niveau de risque acceptable, il peut être nécessaire d'adopter des mesures de gestion des risques.	• L'étude d'impact doit être réalisée dès la phase de conception. • Il convient également d'adopter un processus de conformité se déployant tout au long du cycle de vie du SIA.

10. Une étude d'impact à réaliser dès la phase de conception du SIA. L'étude d'impact sur les VUE doit être réalisée dès la phase de conception du SIA, avant même les phases de vérification et de validation, de déploiement et d'exploitation et de suivi. Plus précisément, l'étude d'impact devrait être effectuée lors de la planification et de la conception du SIA, c'est-à-dire au moment de « la définition du concept et des objectifs du système, des principes sous-jacents, du contexte et du cahier des charges, ainsi que la construction éventuelle du prototype »[2].

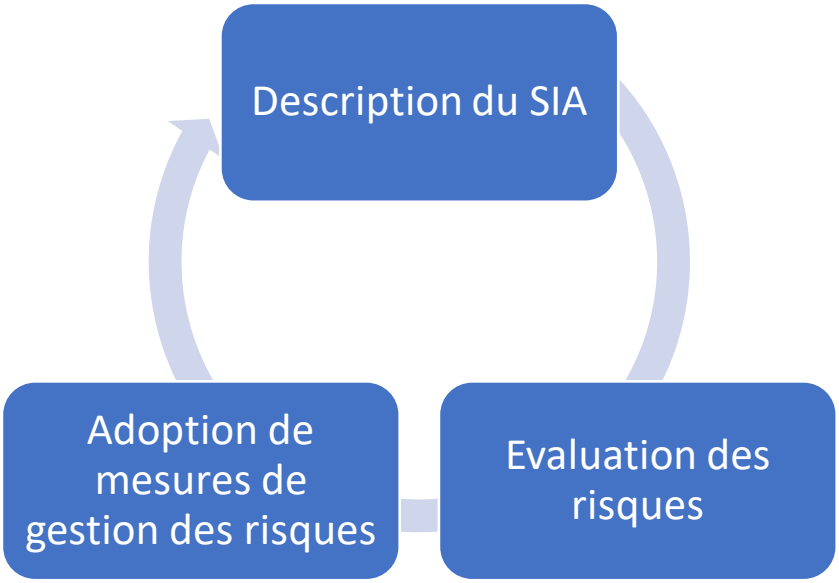


11. Les différentes étapes de l'étude d'impact et leur articulation. L'étude d'impact est divisée en trois étapes principales :

- la première étape repose sur l'identification des risques pour les VUE ;
- la seconde étape a pour objectif l'évaluation de ces risques ;
- la troisième et dernière étape consiste à déterminer les mesures de gestion des risques devant être mises en place.

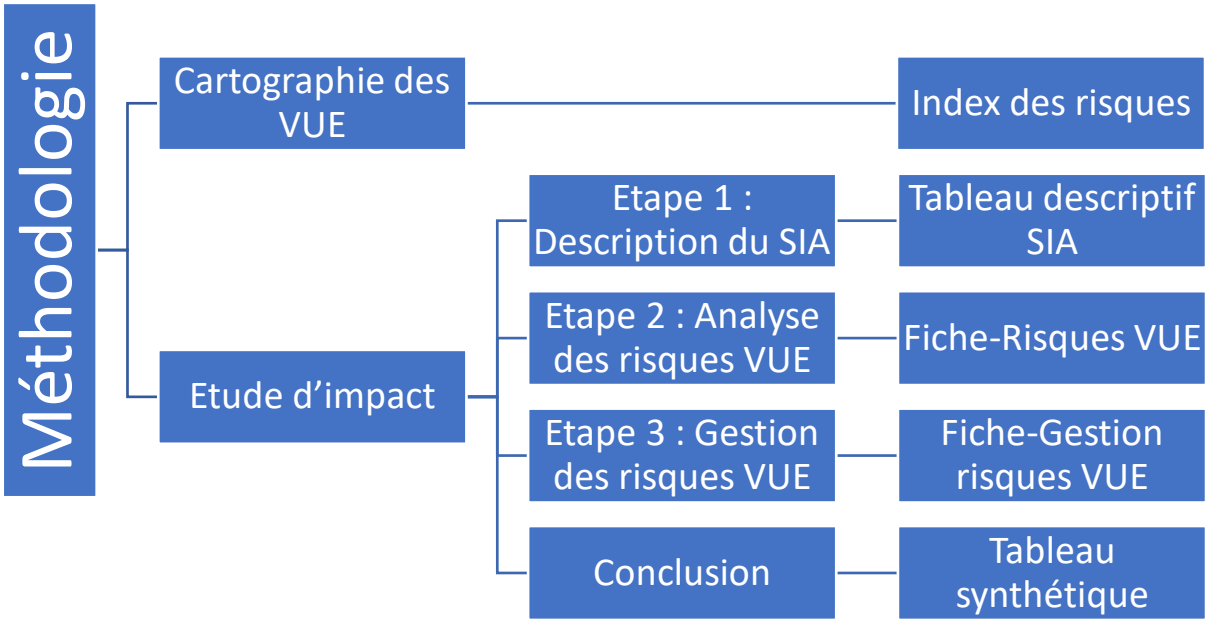
La méthode de réalisation de ces différentes étapes est détaillée dans la partie du Guide intitulée « Boîte à outils ».

Ces trois étapes entretiennent des liens les unes avec les autres et doivent être réalisées dans l'ordre. Ces étapes doivent être répétées tant que le respect des VUE n'est pas en mesure d'être garanti.



12. La nécessité de prévoir un maintien de la conformité tout au long du cycle de vie du SIA. Si l'étude d'impact doit être réalisée dès la conception du SIA, il convient également de garantir le maintien du niveau de conformité tout au long du cycle de vie du SIA, c'est-à-dire après son déploiement, durant sa phase d'exploitation et jusqu'à son arrêt.

13. Méthodologie : l'articulation entre la méthode et les documents pratiques. A chaque étape est attaché une méthode, présentée dans la partie Boîte à outils, et un ou plusieurs documents pratiques dans les annexes. Ces deux éléments ont vocation à être utilisés de concert, la méthodologie expliquant la démarche à suivre et les documents pratiques mettant en œuvre cette démarche.



14. La nécessité d'un dialogue entre le fournisseur et le déployeur : la distinction entre la destination et les finalités. Il est important de préciser la différence terminologique entre la destination du SIA et ses finalités, ainsi que ses implications. La destination est définie par l'AI Act comme « l'utilisation à laquelle un système d'IA est destiné par le fournisseur, y compris le contexte et les conditions spécifiques d'utilisation, tels qu'ils sont précisés dans les informations communiquées par le fournisseur dans la notice d'utilisation, les indications publicitaires ou de vente et les déclarations, ainsi que dans la documentation technique » (AI Act, art. 3, §12). La destination est donc définie par le fournisseur. La finalité, quant à elle, correspond aux besoins du déployeur, les raisons pour lesquelles il souhaite avoir recours à ce SIA spécifique. Idéalement, il conviendrait de prendre en compte la finalité du SIA dans l'étude d'impact. Ceci implique un dialogue entre le fournisseur et le déployeur, afin d'identifier clairement la finalité du SIA pour ce dernier, mais aussi de déterminer en amont le contexte de déploiement du SIA, lequel a des répercussions importantes pour le respect des VUE.

Néanmoins, le fournisseur peut développer un SIA sans avoir de connaissance précise des finalités motivant le déployeur, par exemple s'il n'a pas de commande du déployeur ou si le SIA est destiné à être commercialisé par un distributeur. Dans ce cas, la destination sera le critère premier utilisé dans l'étude d'impact.

Il convient de préciser que l'AI Act impose aux fournisseurs de prendre en compte la « mauvaise utilisation raisonnablement prévisible ». Cette notion est définie par l'article 3, §13 de l'AI Act comme « l'utilisation d'un système d'IA d'une manière qui n'est pas conforme à sa destination, mais qui peut résulter d'un comportement humain raisonnablement prévisible ou d'une interaction raisonnablement prévisible avec d'autres systèmes, y compris d'autres systèmes d'IA ». Il faut alors non seulement prendre en compte les usages conformes à la destination du SIA mais aussi les autres usages pouvant découler des fonctions du SIA. Il est

alors nécessaire de décrire le SIA au regard de sa destination mais aussi des mauvaises utilisations raisonnablement prévisibles par un déployeur potentiel.

2. La portée du Guide pratique

15. L'absence de valeur juridique du Guide. Le présent Guide est un instrument volontaire permettant de favoriser le respect des VUE par les fournisseurs dès la conception et tout au long du cycle de vie d'un SIA. Il ne s'agit pas d'un document officiel émanent d'un État ou de l'Union européenne. Il n'a ni la valeur juridique d'une norme contraignante (loi) ni celle n'une norme technique ou de droit souple (code de conduite par exemple).

Ce Guide doit être distingué de documents légaux comme l'analyse d'impact sur les droits fondamentaux prévue par l'article 27 de l'AI Act, qu'il ne remplace pas.

La mise en œuvre de ce Guide ne constitue pas une cause d'exonération de responsabilité civile, administrative ou pénale des opérateurs de SIA. Le respect de ce Guide ne saurait en outre être considéré comme valant présomption de conformité à tout ou partie de l'AI Act.

Enfin, si l'application de ce Guide pratique favorise le respect des VUE et peut permettre de limiter les risques juridiques, elle ne les supprime pas.

---

[1] Selon l'AI Act, une modification substantielle est une « modification apportée à un système d'IA après sa mise sur le marché ou sa mise en service, qui n'est pas prévue ou planifiée dans l'évaluation initiale de la conformité réalisée par le fournisseur et qui a pour effet de nuire à la conformité de ce système aux exigences énoncées au chapitre III, section 2, ou qui entraîne une modification de la destination pour laquelle le système d'IA a été évalué » (AI Act, art. 3, §23).

[2] Ces quatre phases et leurs éléments constitutifs sont détaillés dans un document de l'OCDE basé sur les travaux du Groupe de travail sur la gouvernance de l'intelligence artificielle (AIGO) : OCDE, *L'intelligence artificielle dans la société*, Paris : Editions OCDE, 2019, p. 28-29

II. Boîte à outils du Guide pratique

A. La cartographie des valeurs de l'Union européenne (annexe 3)

16. Présentation de la cartographie dynamique. La cartographie dynamique des valeurs de l'Union européenne (VUE) a un double objectif.

D'une part, elle permet de connaître ces valeurs dans leur matérialité : leur sens, les hypothèses d'application et leur portée juridique, en particulier à l'aune de leur concrétisation par certains droits et principes fondamentaux. A cette fin, il s'agit de répertorier ces valeurs et les droits et principes fondamentaux qui y sont attachés, sur le fondement de l'article 2 du Traité sur l'Union européenne (TUE), de la Charte des droits fondamentaux de l'Union européenne (la Charte) mais aussi de la Convention européenne des droits de l'Homme (conv. EDH), à laquelle l'Union européenne (l'Union) se réfère, ainsi qu'à la jurisprudence. Cette cartographie n'est pas exhaustive mais présente certaines des valeurs les plus susceptibles d'être mises en tension dans le contexte de systèmes d'IA (SIA) à haut risque dans le domaine industriel, à savoir les valeurs de dignité humaine, de liberté et d'égalité.

D'autre part, elle vise à mettre en lumière les risques d'atteinte que le déploiement d'un SIA à haut risque pourrait causer à ces valeurs et aux droits et principes fondamentaux les concrétisant. Sur cette base, un *Index des risques VUE*, présenté dans l'annexe 3, a été établi. Il prend appui sur les facteurs de risques analysés au sein de la cartographie dynamique des VUE. Cet index est un document de référence nécessaire à la réalisation de l'étude d'impact d'un SIA donné sur les VUE (et notamment la deuxième étape relative à l'identification des risques).

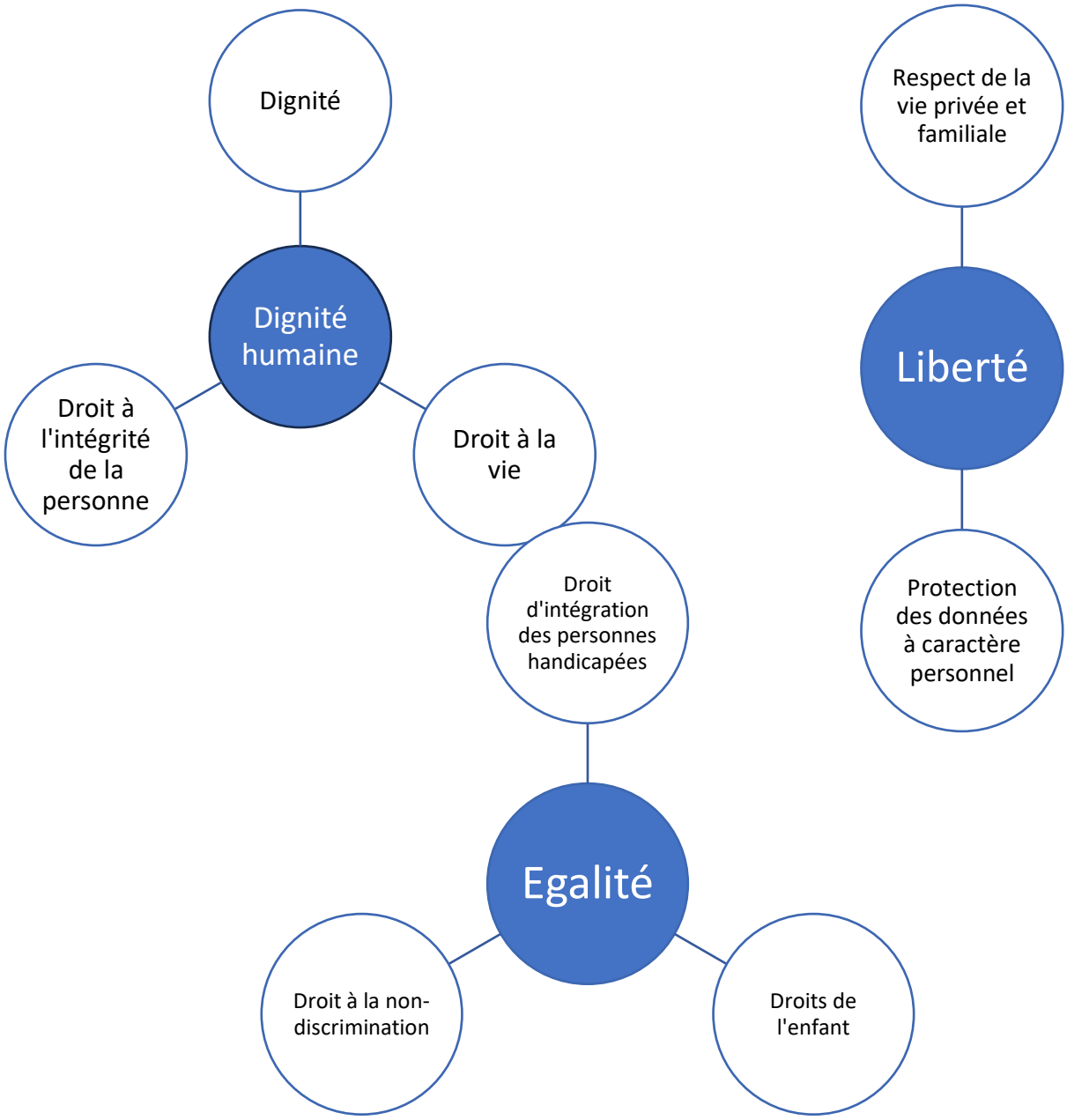
Liste des VUE et des droits et principes fondamentaux de concrétisation
En gras et souligné, les VUE et les droits fondamentaux de concrétisation analysés dans le Guide

VUE	Droits et principes fondamentaux de concrétisation tirés de la Charte des droits fondamentaux de l'Union européenne
Dignité humaine	**Art. 1er – Dignité humaine**
	Art. 2 – Droit à la vie
	Art. 3 – Droit à l'intégrité de la personne
	Art. 4 – Interdiction de la torture et des peines ou traitements inhumains
	Art. 34 – Sécurité sociale et aide sociale
Liberté	Art. 6 – Droit à la liberté et à la sûreté
	Art. 7 – Respect de la vie privée et familiale
	Art. 8 – Protection des données à caractère personnel
	Art. 9 – Droit de se marier et droit de fonder une famille
	Art. 10 – Liberté de pensée, de conscience et de religion
	Art. 11 – Liberté d'expression et d'information

	Art. 12 – Liberté de réunion et d'association
	Art. 13 – Liberté des arts et des sciences
	Art. 14 – Droit à l'éducation
	Art. 15 – Liberté professionnelle et droit de travailler
	Art. 16 – Liberté d'entreprise
	Art. 17 – Droit de propriété
	Art. 18 – Droit d'asile
	Art. 19 – Protection en cas d'éloignement, d'expulsion et d'extradition
	Art. 27 – Droit à l'information et à la consultation des travailleurs au sein de l'entreprise
	Art. 28 – Droit de négociation et d'actions collectives
	Art. 29 – Droit d'accès aux services de placement
	Art. 30 – Protection en cas de licenciement injustifié
	Art. 31 – Conditions de travail justes et équitables
	Art. 32 – Interdiction du travail des enfants et protection des jeunes au travail
	Art. 33 – Vie familiale et vie professionnelle
	Art. 36 – Accès aux services d'intérêt économique général
	Art. 37 – Protection de l'environnement
	Art. 38 – Protection des consommateurs
	Art. 45 – Liberté de circulation et de séjour
Démocratie	Art. 39 – Droit de vote et d'éligibilité aux élections au Parlement européen
	Art. 40 – Droit de vote et d'éligibilité aux élections municipales
	Art. 41 – Droit à une bonne administration
	Art. 42 – Droit d'accès aux documents
	Art. 43 – Médiateur européen
	Art. 44 – Droit de pétition
Egalité	Art. 20 – Egalité en droit
	Art. 21 – Non-discrimination
	Art. 22 – Diversité culturelle, religieuse et linguistique
	Art. 23 – Egalité entre femmes et hommes
	Art. 24 – Droits de l'enfant
	Art. 25 – Droit des personnes âgées
	Art. 26 – Intégration des personnes handicapées
	Art. 35 – Protection de la santé
Etat de droit	Art. 20 – Egalité en droit
	Art. 47 – Droit à un recours effectif et à accéder à un tribunal impartial
	Art. 48 – Présomption d'innocence et droits de la défense

	Art. 49 – Principes de légalité et de proportionnalité des délits et des peines
	Art. 50 – Droit à ne pas être jugé ou puni pénalement deux fois pour une même infraction
	Art. 52 – Portée et interprétation des droits et des principes
	Art. 54 – Interdiction de l'abus de droit
Respect des droits de l'Homme	Art. 22 – Diversité culturelle, religieuse et linguistique
	Art. 53 – Niveau de protection

Droits étudiés dans le Guide :



1. La dignité humaine

17. La dignité humaine : une notion juridique. La dignité, concept primordialement philosophique[3], n'a été érigée que récemment en tant que notion juridique par son intégration dans des textes législatifs, conventionnels ou constitutionnels[4]. En droit de l'Union, la dignité, ou plus précisément le « le respect de la dignité humaine » est la première des valeurs de l'Union, telles qu'énumérées à l'article 2 du TUE. Cette notion apparaît également dans la Charte, la « Dignité » constituant son titre premier. La notion de « dignité humaine » a des acceptions différentes en fonction des ordres juridiques de référence ; la conception française de la dignité, par exemple, ne saurait être assimilée aux conceptions allemande, italienne ou espagnole[5]. Il en est de même pour la conception européenne, qui doit être distinguée de celle des ordres juridiques nationaux des États membres.

18. Les deux principes de la dignité humaine : l'interdiction de la réification des personnes et la satisfaction des besoins vitaux des personnes. Selon le Professeur Muriel Fabre-Magnan, « le principe de dignité exige, pour reprendre la formule du Conseil constitutionnel français, de sauvegarder la personne humaine '' contre toute forme d'asservissement et de dégradation ''. L'impératif se décline en plusieurs principes, qui sont des règles de droit positif directement applicables »[6]. La dignité implique, d'une part, l'interdiction de la réification de la personne. La personne humaine doit être vue comme une fin et non pas utilisée comme un moyen. Ceci implique notamment la prohibition de l'esclavage et du travail forcé[7]. En ce sens, la Commission européenne a indiqué que la dignité humaine consiste à « protéger la personne humaine contre le fait d'être traitée comme un simple objet par l'État ou par ses concitoyens »[8]. Le principe de dignité consiste, d'autre part, à assurer « les besoins vitaux de la personne humaine »[9] : se loger, se nourrir, s'habiller et prendre soin de son hygiène[10].

19. L'absence de définition précise en droit de l'Union. Le droit de l'Union ne définit pas précisément la notion de dignité humaine : en premier lieu parce qu'historiquement l'Union s'est « construite autour de seules notions économiques »[11] ; en second lieu car « une définition précise risquerait de heurter les conceptions nationales »[12]. Par référence à la définition donnée précédemment, la dignité humaine en droit de l'Union pourrait être interprétée comme un concept visant « à empêcher que les personnes ne puissent être réifiées »[13] et à garantir les besoins vitaux de la personne humaine[14].

20. Les droits et principes fondamentaux de concrétisation. La dignité humaine, en tant que VUE, est concrétisée par divers droits et principes fondamentaux. Dans le contexte de l'IA, les plus pertinents semblent être la dignité humaine en tant que droit fondamental (a), le droit à vie (b) et le droit à l'intégrité de la personne (c). Ils apparaissent en effet comme pouvant être menacés par le déploiement d'un SIA à haut risque.

a. La dignité humaine en tant que droit fondamental (art. 1er de la Charte)

> *CHARTE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE*
> *ARTICLE 1 - DIGNITE HUMAINE*
> *LA DIGNITE HUMAINE EST INVIOLABLE. ELLE DOIT ETRE RESPECTEE ET PROTEGEE.*

i. Le cadre juridique

21. La protection des personnes hautement vulnérables. L'article 1er de la Charte consacre la dignité humaine en tant que droit fondamental. La dignité humaine est donc à la fois une VUE et un droit fondamental. On peut toutefois distinguer ces deux références sur le terrain juridique. Comme exposé plus haut, la VUE « dignité humaine » est définie largement et de façon abstraite comme l'interdiction de traiter les personnes comme des choses et l'obligation d'assurer aux personnes la satisfaction de leurs besoins vitaux. Quant à la dignité humaine, droit fondamental, elle est utilisée par le droit dérivé de l'Union et par la Cour de justice de l'Union européenne (CJUE) à des fins de sauvegarde de la personne en situation de grande vulnérabilité au sens où ses besoins vitaux pourraient ne pas être satisfaits (privation de liberté ou du droit de circuler, situation d'insécurité économique et/ou politique, etc.). Ains, la dignité humaine trouve à s'appliquer afin de protéger les détenus[15], des personnes poursuivies[16] ou encore des demandeurs d'asile[17]. Dans ces hypothèses, la Cour de justice apprécie notamment les conditions de vie des personnes et s'assure qu'elles aient accès aux ressources et installations leur permettant de satisfaire leurs besoins vitaux.

La notion de dignité humaine sert également à définir la notion d'aide sociale[18] ou celle de harcèlement moral[19]. La notion de dignité humaine a, en outre, été appliquée pour justifier l'interdiction de jeux de simulation d'actes homicides[20].

ii. Les risques d'atteinte par les SIA

22. Premier facteur de risque : la grande vulnérabilité. Un SIA pourrait porter atteinte à la dignité humaine, comme droit fondamental, lorsqu'il est utilisé dans le cadre de la prise de décisions relatives à des personnes particulièrement vulnérables, par exemple s'agissant d'une décision administrative d'accès au territoire d'un État en droit des étrangers ou d'une décision déterminant le montant d'une prestation sociale destinée à une famille monoparentale. Cette vulnérabilité doit notamment être entendue dans le sens d'une vulnérabilité exogène c'est-à-dire une vulnérabilité sociale ou économique[21]. La dignité humaine « pourra être affectée ou atteinte chaque fois qu'un système d'IA aura privé ou restreint une personne d'un élément qui lui est indispensable ou inhérent à sa nature » comme l'accès à la nourriture, à un logement ou à la santé[22].

D'une façon générale, l'AI Act prohibe l'*exploitation des vulnérabilités des personnes* liées à leur âge (par exemple, les mineurs), leurs handicaps ou leur situation économique ou sociale (extrême pauvreté, appartenance à une minorité religieuse ou ethnique). L'utilisation de SIA visant des catégories de personnes vulnérables ayant pour but ou pour effet de modifier leurs comportements de façon préjudiciable est interdite par l'AI Act (AI Act, art. 5, §1, sous b).

Plus spécifiquement, il existe un risque d'atteinte lorsque le SIA est utilisé pour déterminer les conditions de vie d'une *personne détenue* ou *retenue* et notamment ses conditions matérielles de vie (accès à un logement, à la nourriture ou à l'habillement) ou son droit à travailler. Il existe également un risque lorsque le SIA est utilisé pour déterminer le droit ou le montant de *prestations sociales* ou encore l'accès au *logement*, à l'*électricité* ou aux *télécommunications* ou aux *services d'urgence*.

Il faut noter que l'AI Act prévoit des dispositions spécifiques pour l'utilisation de l'IA dans les domaines de l'immigration, des demandes d'asile et du contrôle aux frontières dans la mesure où des personnes particulièrement vulnérables peuvent être concernées (AI Act, cons. 60, art. 6, §2 et annexe III, pt 7). Sont ainsi classés à haut risque, et sont susceptibles de porter atteinte à la dignité, les SIA utilisés en tant que *polygraphes* ou pour l'*évaluation du risque que représente une personne* (risque pour la sécurité, de migration irrégulière ou pour la santé).

23. Second facteur de risque : la note sociale. Enfin, l'AI Act considère expressément que l'évaluation ou la classification des personnes basées sur leurs pratiques sociales, c'est-à-dire, l'établissement d'une *note sociale*, peut être contraire à la dignité humaine car il peut conduire à des discriminations et à l'exclusion de certains groupes de personnes (AI Act, art. 5, §1, c).

b. Le droit à la vie (art. 2 de la Charte)

> *CHARTE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE*
> *ARTICLE 2 - DROIT A LA VIE*
> *1. TOUTE PERSONNE A DROIT A LA VIE.*
> *2. NUL NE PEUT ETRE CONDAMNE A LA PEINE DE MORT, NI EXECUTE.*

i. Le cadre juridique

24. Les dimensions négative et positive du droit à la vie. Le droit à la vie consacré par la Charte a deux dimensions, l'une négative, l'autre positive, à l'image du droit consacré par l'article 2 de la Convention européenne des droits de l'Homme. Dans sa dimension négative, le droit à la vie implique l'interdiction pour les États de donner volontairement la mort et dans sa dimension positive, il oblige les États « à prendre les mesures nécessaires à la protection de la vie des personnes »[23].

25. La protection des personnes vulnérables. Ainsi que cela ressort de la jurisprudence européenne, le droit à la vie vise en particulier à protéger les personnes se trouvant dans des situations de particulière vulnérabilité comme les personnes détenues[24] ou les demandeurs d'asile[25] ou les étrangers dont la vie serait menacée en cas d'expulsion[26] ou encore les personnes handicapées[27]. Le droit à la vie implique notamment l'obligation pour les États de prodiguer les soins appropriés aux personnes et de mettre en place les enquêtes et procédures permettant de sanctionner les atteintes portées à la vie des personnes.

26. L'environnement. En outre, le droit à la vie peut être associé à des problématiques environnementales[28], à l'instar de l'exposition des personnes à des substances dangereuses. Dans ce cas, la doctrine souligne que « l'État doit mettre en œuvre les ‘‘ réglementations préventives ’’ appropriées et respecter le ‘‘ droit du public à l'information ’’ »[29].

27. Le terrorisme. La question du terrorisme entretient des liens étroits avec le droit à la vie. Le droit à la vie implique l'obligation pour les États de protéger leurs citoyens contre les actes d'homicides, y compris ceux commis par des particuliers. Cette obligation constitue, selon la doctrine, le fondement de la lutte contre le terrorisme[30]. En particulier, l'obligation de

protéger le droit à la vie implique l'obligation pour l'État de prendre en amont les mesures nécessaires pour prévenir la commission d'actes de terrorisme[31].

Le droit de l'Union ne fonde toutefois pas expressément la lutte contre le terrorisme sur le droit à la vie mais, plus largement, sur l'ensemble des valeurs de l'Union[32].

28. Les actions des forces de sécurité. Le droit à la vie encadre l'action des forces de sécurité. En effet, si la protection de la population et la légitime défense peuvent justifier le recours à la force meurtrière par les forces de sécurité, cette atteinte au droit à la vie est encadrée. Ainsi, par exemple, les mesures antiterroristes doivent être organisées de façon à réduire le risque pour la vie. Il en résulte que la mort de personnes soupçonnées de terrorisme lors d'une opération de police peut être considérée comme une violation du droit à la vie si le décès de ces personnes est la conséquence d'une planification insuffisante de l'opération par les autorités[33].

29. La peine de mort. La garantie du droit à la vie implique la prohibition de la peine de mort ; il s'agit d'un acquis partagé au sein des États membres de l'Union. Pour autant, la question contenue à se poser sous l'angle de l'exportation hors de l'Union de produits européens destinés à mettre en œuvre une peine de mort dans un État qui la pratique. Sur le fondement, entre autres, de l'article 2 paragraphe 2 de la Charte, le règlement 2019/125 du 16 janvier 2019 concernant le commerce de certains biens susceptibles d'être utilisés en vue d'infliger la peine capitale, la torture ou d'autres peines ou traitements cruels, inhumains ou dégradants encadre le commerce de ces biens. Le régime dépend de la destination du bien. Plus précisément, il faut distinguer les biens n'ayant aucune autre utilisation pratique que celle d'infliger la peine capitale, la torture et d'autres peines ou traitements cruels, inhumains ou dégradants, les biens susceptibles d'être utilisés en vue d'infliger la torture ou d'autres peines ou traitements cruels, inhumains ou dégradants et les biens susceptibles d'être utilisés en vue d'infliger la peine capitale. Pour la première catégorie de biens, la règle est celle de l'interdiction de l'exportation et l'importation, du transit, du courtage, de la publicité ou de la présentation dans les salons professionnels. Les deux autres catégories de biens sont soumises à un régime d'autorisation.

30. L'exception au droit à la vie : les actes licites de guerre. Enfin, il faut préciser que « le droit à la vie est un droit absolu, indérogeable, à la seule exception de celle qui est prévue à l'article 15, paragraphe 2, de la Convention européenne des droits de l'homme, à savoir ''le cas de décès résultant d'actes licites de guerre'' »[34]. En effet, alors même que le droit international humanitaire impose, en principe, le respect des droits de l'Homme durant les conflits armés, il existe certaines exceptions lorsque les États ont déclaré un état de guerre.

ii. Les risques d'atteinte par les SIA

31. Premier facteur de risque : le dispositif de sécurité. Un SIA peut porter atteinte au droit à la vie lorsque son utilisation est susceptible d'entraîner directement ou indirectement la mort d'une personne.

D'un point de vue général, ce peut être le cas lorsqu'un SIA, utilisé en tant que *dispositif de sécurité*, est défaillant et menace alors la vie des personnes (par ex. risque d'endommagement de matériel garantissant la sécurité sanitaire ; ou défaillance d'un SIA dans un véhicule, autonome ou non, pouvant provoquer un accident mortel). A l'aune de l'AI Act,

on peut citer l'exemple des dispositifs de sécurité d'infrastructures critiques qui, comme le note l'AI Act, dont la défaillance ou le mauvais fonctionnement pourraient « directement entraîner des risques pour l'intégrité physique des infrastructures critiques et, partant, des risques pour la santé et la sécurité des personnes et des biens » (AI Act, cons. 55), à l'instar des systèmes de surveillance de la pression de l'eau ou des systèmes de commande des alarmes incendie dans les centres d'informatique en nuage.

C'est également le cas des dispositifs de sécurité des *équipements médicaux* – qui entrent également dans le champ d'application de l'AI Act, en tant que législation d'harmonisation (AI Act, cons. 50 et annexe I, pt 11 et 12) – dont la défaillance peut avoir de graves répercussions sur la santé des personnes.

32. Deuxième facteur de risque : la grande vulnérabilité. Le SIA peut également être lié à un risque pour le droit à la vie lorsqu'il est utilisé dans le cadre d'une décision concernant une personne particulièrement vulnérable. Cela pourrait être le cas d'un *étranger* dont la vie serait menacée par une mesure d'expulsion fondée sur un dispositif d'IA et ce, eu égard aux conditions particulièrement dangereuses auxquelles il serait exposé en cas de retour dans son État d'origine (AI Act, cons. 60, art. 6, §2 et annexe III, pt 7).

33. Troisième facteur de risque : l'armement. On peut s'interroger sur l'utilisation d'armes associées à un SIA (systèmes d'armes létaux autonomes ou SALA) ou de SIA destinés à fournir une assistance à l'usage d'*armes*. Cette utilisation peut être prévue ou prévisible par le fournisseur ou résulter d'un détournement de l'utilisation du SIA ; dans tous les cas, elle est exclue de l'AI Act qui n'est pas applicable en matière de sécurité nationale et à l'égard de SIA utilisés « exclusivement à des fins militaires, de défense ou de sécurité nationale » (AI Act, art. 2, §3).

Tout d'abord, l'utilisation de tels robots pour exécuter une *peine de mort* porterait atteinte au droit à la vie. Ensuite, concernant l'utilisation de SALA ou de SIA destinés à fournir une assistance au tir, il faut distinguer l'usage dans un contexte de guerre ou dans un contexte de paix. Dans le premier cas, le droit à la vie ne protège pas les militaires, qui ont abandonné le bénéfice de ce droit[35], mais protège les civils. Ainsi, le risque d'atteinte à la vie existe à l'égard des civils lorsque le SIA est destiné à un usage militaire. Dans le second cas, le droit à la vie encadre l'action des *agents de l'Etat* vis-à-vis de l'ensemble de la société.

c. Le droit à l'intégrité de la personne (art. 3 de la Charte)

CHARTE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE

ARTICLE 3 - DROIT A L'INTEGRITE DE LA PERSONNE

1. TOUTE PERSONNE A DROIT A SON INTEGRITE PHYSIQUE ET MENTALE.

2. DANS LE CADRE DE LA MEDECINE ET DE LA BIOLOGIE, DOIVENT NOTAMMENT ETRE RESPECTES

A) LE CONSENTEMENT LIBRE ET ECLAIRE DE LA PERSONNE CONCERNEE, SELON LES MODALITES DEFINIES PAR LA LOI ;

B) L'INTERDICTION DES PRATIQUES EUGENIQUES, NOTAMMENT CELLES QUI ONT POUR BUT LA SELECTION DES PERSONNES ;

C) L'INTERDICTION DE FAIRE DU CORPS HUMAIN ET DE SES PARTIES, EN TANT QUE TELS, UNE SOURCE DE PROFIT ;

D) L'INTERDICTION DU CLONAGE REPRODUCTIF DES ETRES HUMAINS.

i. Dans un cadre général

• Le cadre juridique

34. La définition de la protection de l'intégrité physique et mentale. L'article 3 de la Charte protège l'intégrité physique et mentale de la personne. D'une part, la protection de l'intégrité physique vise à protéger le corps de la personne. Plus précisément, il s'agit de protéger la personne contre des dommages corporels. La mort ne semble pas devoir être considérée comme une atteinte au droit à l'intégrité physique mais comme un atteinte au droit à la vie, protégé par l'article 2[36]. Le droit à l'intégrité physique implique pour les États d'adopter des mesures juridiques visant à la protéger[37].

D'autre part, la protection de l'intégrité mentale vise à protéger la personne contre des souffrances morales ou psychologiques. Il s'agit notamment de la protéger contre des traitements « inhumains » ou « dégradants »[38].

• Les risques d'atteinte par les SIA

35. Premier facteur de risque : le dispositif de sécurité. Les SIA sont notamment susceptibles de porter atteinte au droit à l'intégrité physique lorsqu'ils sont utilisés en tant que *dispositifs de sécurité*. Par exemple, la défaillance d'un SIA embarqué dans un véhicule peut avoir pour conséquence de provoquer un accident causant un dommage corporel. On peut également citer le cas des *dispositifs de sécurité de la gestion et de l'utilisation d'infrastructures critiques* (AI Act, annexe II, pt. 2) destinés à garantir l'accès aux personnes à des biens et services essentiels et à préserver la sécurité des populations.

36. Deuxième facteur de risque : les techniques subliminales. L'utilisation de *techniques subliminales* destinées à manipuler le comportement des personnes les privant ainsi de leur autonomie et portant atteinte à leur intégrité mentale peut être considéré comme contraire à la dignité humaine. Ces pratiques sont interdites par l'AI Act (AI Act, cons. 29 et art. 5, §1, a). Il s'agit de techniques pouvant notamment être mises en œuvre grâce à des *interfaces cerveau-machine* ou la *réalité virtuelle*.

37. Troisième facteur de risque : la détection et la reconnaissance des émotions. L'utilisation de SIA de *détection et de reconnaissance des émotions* fait l'objet de nombreuses réserves, notamment en raison de leur insuffisante fiabilité[39]. L'AI Act encadre ainsi leur utilisation, interdisant l'usage de tels SIA dans le cadre d'une relation de travail et scolaire. En revanche, il est possible d'y avoir recours à des fins de sécurité ou médicales (AI Act, art. 5, §1, f).

38. Quatrième facteur de risque : l'hypertrucage. L'*image* ou la *voix* des personnes peut être utilisée d'une façon portant atteinte à leur intégrité morale. Le risque est que l'image ou la voix des personne soient utilisées pour créer des contenus portant atteinte à leur honneur grâce à des outils de *deepfake* ou d'*hypertrucage*. L'hypertrucage est défini par l'article 3, §60 de l'AI Act comme « une image ou un contenu audio ou vidéo généré ou manipulé par l'IA, présentant une ressemblance avec des personnes, des objets, des lieux, des entités ou événements existants et pouvant être perçu à tort par une personne comme authentiques ou véridiques ».

Il faut porter une attention particulière à l'image des *enfants*. La directive 2011/93 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants prévoit un régime de protection spécifique de l'image des enfants. L'article 2, c) de la directive définit la pédopornographie comme la représentation d'enfants ou d'images réalistes d'enfants à des fins principalement sexuelles. Un SIA pourrait être utilisé afin de créer de tels contenus illicites. Mais plus généralement, la création de contenus pornographiques utilisant l'image ou la voix d'une personne sans son consentement doit être considérée comme une pratique interdite, portant atteinte à son intégrité morale.

On notera à ce sujet que l'AI Act prévoit un encadrement de ce type de SIA (AI Act, art. 50, §4).

ii. L'application particulière dans le cadre de la médecine et de la biologie

• Le cadre juridique

39. Les quatre principes applicables à la médecine et à la biologie. La médecine et la biologie sont des activités portant par nature atteinte à l'intégrité physique et mentale des personnes. Par exemple un acte de chirurgie constitue une atteinte à l'intégrité physique légitime. Dans ces conditions, il s'avère nécessaire de prévoir des dispositions spéciales. A cette fin, le paragraphe 2 de l'article 3 de la Charte contient des dispositions visant spécifiquement la médecine et la biologie. Il s'agit du domaine de la bioéthique.

Le paragraphe 2 énonce quatre principes, non exhaustifs[40], applicables aux activités médicales et biologiques. En premier lieu, il est exigé de respecter « le consentement libre et éclairé de la personne concernée, selon les modalités définies par la loi ». Concernant ce consentement, le droit français (sur la base de l'article L. 4001-3 du code de la santé publique) encadre l'utilisation de l'intelligence artificielle par les professionnels de santé en imposant une obligation d'information du patient, une accessibilité aux données et une obligation d'explicabilité du traitement algorithmique[41]. En second lieu, la Charte prévoit l'interdiction des « pratiques eugéniques, notamment celles qui ont pour but la sélection des personnes. En troisième lieu, est posée « l'interdiction de faire du corps humain et de ses parties, en tant que tels, une source de profit ». En dernier lieu, « l'interdiction du clonage reproductif des êtres humains » est prévue.

• Les risques d'atteinte par les SIA

40. Premier facteur de risque : les manipulations génétiques. Les SIA peuvent être utilisés afin de réaliser des *manipulations génétiques* sur les gamètes et les embryons. Ces manipulations génétiques sont encadrées par la loi. En droit français par exemple, l''article L. 511-1 du code pénal interdit le clonage des personnes consistant au « fait de se prêter à un prélèvement de cellules ou de gamètes, dans le but de faire naître un enfant génétiquement identique à une autre personne, vivante ou décédée ».

41. Deuxième facteur de risque : les neuro-technologies. Les *neuro-technologies* ont pour objectif de modifier le comportement du cerveau humain. Associées à l'IA, elles peuvent permettre d'améliorer les méthodes de thérapie comportementale et cognitive

destinées à soigner les troubles psychiques. Néanmoins, comme le souligne l'Unesco, ces technologies présentent des risques pour les personnes. D'une part, l'utilisation à des fins commerciales peut menacer l'autonomie des individus et, d'autre part, l'accès à ces technologies peut accentuer des inégalités sociales[42]. En ce sens, comme évoqué plus haut, l'AI Act interdit certaines pratiques en matière d'IA qui altèrent le fonctionnement neurologique des personnes (cons. 29 et art. 5, §1 s'agissant des techniques subliminales préc.).

[3] NERI Kiara, « La notion de dignité humaine, fondement de l'émergence de nouveaux droits de l'homme ou nouveau droit substantiel ? » *In* DOUMBE-BILLE Stéphane (dir.), *Nouveaux droits de l'homme et internationalisation du droit*, Bruxelles :Bruylant, coll. Cahiers de droit international, 2012

[4] FABRE-MAGNAN Muriel, « La dignité en Droit : un axiome », *Revue interdisciplinaire d'études juridiques*, 2007/1 (Volume 58), pp. 3 et s.

[5] V. par ex. les différentes contributions dans BURGORGUE-LARSEN Laurence (dir.), *La dignité saisie par les juges en Europe*, Bruxelles : Bruylant, coll. Droit et justice, 2011

[6] FABRE-MAGNAN Muriel, « La dignité en Droit : un axiome », *Revue interdisciplinaire d'études juridiques*, 2007/1 (Volume 58), p. 25

[7] FABRE-MAGNAN Muriel, « La dignité en Droit : un axiome », *Revue interdisciplinaire d'études juridiques*, 2007/1 (Volume 58), pp. 25-26

[8] Commission européenne, *Rapport 2010 sur l'application de la charte des droits fondamentaux de l'Union européenne*, Luxembourg : Office des publications de l'Union européenne, 2011, p. 21

[9] FABRE-MAGNAN Muriel, « La dignité en Droit : un axiome », *Revue interdisciplinaire d'études juridiques*, 2007/1 (Volume 58), pp. 26-27 ; CHEYNET DE BEAUPRE Aline, « Intelligence artificielle & droit au respect de la dignité humaine » *In* BARBE Vanessa *et al*. (dir.), *Intelligence artificielle & droits fondamentaux*, Toulouse : Éditions L'Épitoge, coll. L'Unité du droit, 2022, p.32

[10] CJUE, 1er août 2022, Ministero dell'Interno c/ TO, aff. C-422/21

[11] FABRE-MAGNAN Muriel, « La dignité en Droit : un axiome », *Revue interdisciplinaire d'études juridiques*, 2007/1 (Volume 58), p. 6

[12] VIAL Claire, « Article 1 Dignité humaine », *In* PICOD Fabrice et RIZCALLAH Cecilia et VAN DROOGHENBROECK Sébastien (dir.), *Charte des droits fondamentaux de l'Union européenne : Commentaire article par article*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 3ème éd., 2023, p. 60

[13] VIAL Claire, « Article 1 Dignité humaine », *In* PICOD Fabrice et RIZCALLAH Cecilia et VAN DROOGHENBROECK Sébastien (dir.), *Charte des droits fondamentaux de l'Union européenne : Commentaire article par article*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 3ème éd., 2023, p. 60

[14] CJUE, 1er août 2022, Ministero dell'Interno c/ TO, aff. C-422/21

[15] CJUE, 5 avril 2016, Aranyosi et Căldăraru, aff. jtes C-404/15 et C-659/15

[16] CJUE, 14 janv. 2021, UC et TD, aff. C-769/19

[17] CJUE, 12 nov. 2019, Haqbin c/ Federaal Agentschap voor de opvang van asielzoekers, aff. C-233/18 ; CJUE, 1er août 2022, Ministero dell'Interno c/ TO, aff. C-422/21 ; CJUE, 14 janv. 2021, K.S. et M.H.K. c/ The International Protection Appeals Tribunal *et al.* et R.A.T. et D.S. c/ Minister for Justice and Equality, aff. jtes C-322/19 et C-385/19

[18] CJUE, 15 septembre 2015, Alimanovic, aff. C-67/14

[19] Trib. UE, 29 juin 2018, HF c/ Parlement, aff. T-218/17

[20] CJCE, 14 oct. 2004, Omega c/ Oberbürgermeisterin der Bundesstadt Bonn, aff. C-36/02

[21] MAUCLAIR Stéphanie, « Intelligence artificielle, droits fondamentaux & personnes vulnérables : une cohabitation sous tension, In BARBE Vanessa *et al.* (dir.), Intelligence artificielle & droits fondamentaux, Toulouse : Éditions L'Épitoge, coll. L'Unité du droit, 2022, p. 74

[22] CHEYNET DE BEAUPRE Aline, « Intelligence artificielle & droit au respect de la dignité humaine » *In* BARBE Vanessa *et al*. (dir.), *Intelligence artificielle & droits fondamentaux*, Toulouse : Éditions L'Épitoge, coll. L'Unité du droit, 2022, p. 32

[23] TULKENS Françoise et VAN DROOGHENBROECK Sébastien, « Article 2 Droit à la vie » *In* PICOD Fabrice et RIZCALLAH Cecilia et VAN DROOGHENBROECK Sébastien (dir.), *Charte des droits fondamentaux de l'Union européenne : Commentaire article par article*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 3ème éd., 2023, p. 76

[24] CEDH, 6 oct. 2008, Renolde c/ France, req. n° 5608/0

[25] CEDH, 27 juil. 2004, Slimani c/ France, req. n° 57671/00
[26] CJUE, 22 nov. 2022, X c/ Staatssecretaris van Justitie en Veiligheid, aff. C-69/21
[27] CEDH, 7 juil. 2014, Centre de ressources juridiques au nom de Valentin Câmpeanu c/ Roumanie, req. n° 47848/08
[28] CEDH, 18 juin 2002, Oneryildiz c/ Turquie, req. n° 48939/99
[29] TULKENS Françoise et VAN DROOGHENBROECK Sébastien, « Article 2 Droit à la vie » *In* PICOD Fabrice et RIZCALLAH Cecilia et VAN DROOGHENBROECK Sébastien (dir.), *Charte des droits fondamentaux de l'Union européenne : Commentaire article par article*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 3ème éd., 2023, p. 83
[30] TULKENS Françoise et VAN DROOGHENBROECK Sébastien, « Article 2 Droit à la vie » *In* PICOD Fabrice et RIZCALLAH Cecilia et VAN DROOGHENBROECK Sébastien (dir.), *Charte des droits fondamentaux de l'Union européenne : Commentaire article par article*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 3ème éd., 2023, p. 84
[31] CEDH, 28 oct. 1998, Osman c/ Royaume-Uni, req. n° 23452/94 ; CEDH, 13 avril 2017, Tagayeva *et al.* c/ Russie, req. n° 26562/07, 14755/08 et 49339/08
[32] En ce sens, le deuxième considérant de la directive 2017/541 relative à la lutte contre le terrorisme (*JOUE,* L 88, 31 mars 2017, p. 6–21) énonce plus largement que « les actes de terrorisme constituent l'une des violations les plus graves des valeurs universelles de dignité humaine, de liberté, d'égalité et de solidarité, ainsi que de jouissance des droits de l'homme et des libertés fondamentales, sur lesquelles l'Union est fondée. Ils représentent également l'une des atteintes les plus graves aux principes de démocratie et d'État de droit, qui sont communs aux États membres et sur lesquels l'Union repose ». Le terrorisme est donc considéré comme contraire à l'ensemble des valeurs de l'Union. Ceci peut notamment s'expliquer par le caractère protéiforme des actes de terrorisme, mis en lumière par l'article 3 de la directive précitée. Les actes de terrorisme peuvent en effet être des homicides mais peuvent également être considérés comme des actes de terrorisme l'enlèvement et la prise d'otage ou encore la destruction massive de biens. Tous les actes de terrorisme ne portent donc pas atteinte au droit à la vie.
[33] CEDH, 27 sept. 1995, McCann *e.a*. c/ Royaume-Uni, req. n° 18984/91. V.TULKENS Françoise et VAN DROOGHENBROECK Sébastien, « Article 2 Droit à la vie » *In* PICOD Fabrice et RIZCALLAH Cecilia et VAN DROOGHENBROECK Sébastien (dir.), *Charte des droits fondamentaux de l'Union européenne : Commentaire article par article*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 3ème éd., 2023, p. 85
[34] TULKENS Françoise et VAN DROOGHENBROECK Sébastien, « Article 2 Droit à la vie » *In* PICOD Fabrice et RIZCALLAH Cecilia et VAN DROOGHENBROECK Sébastien (dir.), *Charte des droits fondamentaux de l'Union européenne : Commentaire article par article*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 3ème éd., 2023, p. 75
[35] NEVEJANS Nathalie, « La légalité des robots de guerre dans les conflits internationaux », *D*., 2016, p. 1273
[36] Par exemple, la position commune 2001/931/PESC du Conseil du 27 décembre 2001 relative à l'application de mesures spécifiques en vue de lutter contre le terrorisme distingue « les atteintes à la vie d'une personne, pouvant entraîner la mort » et « les atteintes graves à l' intégrité physique d'une personne ».
[37] CJUE, 6 oct. 2020, La Quadrature du Net *et al*. c/ Premier ministre *et al*., aff. C-511/18 ; CJUE, 5 avril 2022, G.D. c/ Commissioner of An Garda Síochána *et al*., aff. C-140/20
[38] VANNESTE Frédéric, « Article 3 Droit à l'intégrité de la personne » *In* PICOD Fabrice et RIZCALLAH Cecilia et VAN DROOGHENBROECK Sébastien (dir.), *Charte des droits fondamentaux de l'Union européenne : Commentaire article par article*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 3ème éd., 2023, pp. 99 et s.
[39] V. Défenseur des droits, *Technologies biométriques : l'impératif respect des droits fondamentaux*, 2021.
[40] EU network of independent experts on fundamental rights, *Commentary of the Charter of fundamental rights of the European union*, 2006, p. 38
[41] Art. L.400-3 du code de la santé publique :
« I.-Le professionnel de santé qui décide d'utiliser, pour un acte de prévention, de diagnostic ou de soin, un dispositif médical comportant un traitement de données algorithmique dont l'apprentissage a été réalisé à partir de données massives s'assure que la personne concernée en a été informée et qu'elle est, le cas échéant, avertie de l'interprétation qui en résulte.
II.-Les professionnels de santé concernés sont informés du recours à ce traitement de données. Les données du patient utilisées dans ce traitement et les résultats qui en sont issus leur sont accessibles.
III.-Les concepteurs d'un traitement algorithmique mentionné au I s'assurent de l'explicabilité de son fonctionnement pour les utilisateurs. »
[42] Unesco, *Ethique des neurotechnologies*. Disponible sur : https://www.unesco.org/fr/ethics-neurotech

2. La liberté

42. La liberté et les libertés. La « liberté » doit être distinguée des « libertés » ; « Employé au singulier le mot de liberté semble avoir une portée très large, très généreuse et nettement politique. Il s'agit de garantir la liberté, droit essentiel de l'homme, conquête des régimes politiques démocratiques. Présentées au pluriel, les libertés paraissent recouvrir des réalités plus concrètement et plus modestement '' physiques '' et '' économiques '' »[43].

A ce titre, il faut noter la différence entre l'article 2 du TUE, qui emploie le terme de « liberté », et le chapitre 2 de la Charte intitulé « Libertés ». La liberté, en tant que VUE, « est rarement invoquée dans la jurisprudence de manière générale » et « l'est ordinairement sous les différentes formes dans lesquelles elle se décline », c'est-à-dire sur le fondement des libertés consacrées par la Charte[44].

43. Le principe de liberté. La liberté est un concept fondamental des ordres juridiques européens qui sont fondés sur le libéralisme. Plus précisément, la liberté constitue un principe. Comme l'indique par exemple l'article 5 de la Déclaration des droits de l'Homme et du citoyen de 1789 « tout ce qui n'est pas défendu par la loi ne peut être empêché, et nul ne peut être contraint à faire ce qu'elle n'ordonne pas ». Ainsi, à défaut de règle prohibant un comportement ou l'obligeant, on applique le principe de liberté, c'est-à-dire un principe laissant le choix aux personnes de faire ou ne pas faire une chose.

A la différence de la dignité humaine, qui est selon l'article 1er de la Charte « inviolable », la principe de liberté peut connaître des limitations et les libertés ne sont donc pas droits absolus, que ce soit en droit de l'Union ou dans le droit des États membres. L'article 4 de la Déclaration des droits de l'Homme et du citoyen de 1789 indique que « la liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui » et que « l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres membres de la société la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la loi ». Dans le même sens, le premier alinéa de l'article 2 de la Loi fondamentale allemande dispose que « chacun a droit au libre épanouissement de sa personnalité pourvu qu'il ne viole pas les droits d'autrui ni n'enfreigne l'ordre constitutionnel ou la loi morale ».

Néanmoins, ces limitations sont strictement encadrées et certaines libertés bénéficient d'une protection particulière, comme le révèle les dispositions de la Charte.

44. Les droits et principes fondamentaux de concrétisation. La liberté, en tant que VUE, est concrétisée par divers droits et principes fondamentaux. Dans le contexte de l'IA, les plus intéressants semblent être le droit au respect de la vie privée et familiale (a) et le droit à la protection des données à caractère personnel (b). En effet, l'utilisation de certains SIA peuvent avoir une influence négative sur la jouissance de ces droits par les individus.

a. Le respect de la vie privée et familiale (art. 7 de la Charte)

CHARTE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE

ARTICLE 7 - RESPECT DE LA VIE PRIVEE ET FAMILIALE

TOUTE PERSONNE A DROIT AU RESPECT DE SA VIE PRIVEE ET FAMILIALE, DE SON DOMICILE ET DE SES COMMUNICATIONS.

i. Le cadre juridique

45. La protection de la vie privée. Dans le cadre juridique européen, le respect de la vie privée se voit généralement attribuer une double dimension. La première concerne la protection de l'intimité de la personne contre les immiscions non consenties. La seconde concerne la représentation de la personne dans la sphère sociale, le droit d'avoir une vie privée sociale, d'interagir avec les autres et de s'épanouir[45]. La notion de vie privée recouvre ainsi, en droit de l'Union, à la fois « l'intégrité physique, psychologique et morale de la personne, son identité physique et sociale, mais aussi le droit au développement personnel et le droit d'établir et d'entretenir des rapports avec d'autres êtres humains et le monde extérieur »[46].

Le droit au respect de la vie privée s'applique aux personnes physiques et aux personnes morales[47]. En outre, la protection de la vie privée s'étend au-delà de la sphère de la vie personnelle et inclut la vie professionnelle et commerciale[48].

Quant aux objets auxquels il s'applique, la Cour de justice de l'Union européenne a eu l'occasion de juger que le droit au respect de la vie privée concerne l'image d'une personne[49], ses nom et prénom[50], sa vie intime[51], son état de santé[52] et sa réputation[53]. A ce titre, le droit au respect de la vie privée doit, par exemple et selon la jurisprudence de la Cour de justice, être pris en compte dans le cadre d'une mise en balance des intérêts concernant l'installation d'un dispositif de vidéosurveillance dans les parties communes d'un immeuble à usage d'habitation[54].

46. La protection du domicile. L'article 7 de la Charte confère également une protection du domicile des personnes. La protection du domicile s'entend de l'inviolabilité du domicile[55], qui comprend la protection contre les divulgations du lieu de domicile, les intrusions dans le domicile et la surveillance du domicile[56], qu'il s'agisse d'atteinte par des personnes privées ou par l'autorité publique. Cette protection du domicile est non seulement accordée au domicile de la personne privée mais aussi aux « locaux commerciaux des sociétés »[57], et par extension aux locaux occupés par des personnes morales.

47. La protection des communications. La Cour de justice de l'Union européenne retient une conception large de la notion de communication. Ainsi, elle considère que « les interceptions de télécommunications constituent des ingérences dans l'exercice du droit garanti par l'article 8, paragraphe 1, de la CEDH » et qu' « il en est de même des saisies de courriers électroniques opérées au cours de visites domiciliaires dans des locaux professionnels ou commerciaux d'une personne physique ou dans les locaux d'une société commerciale »[58].

ii. Les risques d'atteinte par les SIA

48. Premier facteur de risque : l'interaction des SIA avec des personnes physiques. La protection de la vie privée implique, on l'a dit, « le droit au développement personnel et le droit d'établir et d'entretenir des rapports avec d'autres êtres humains et le monde extérieur »[59]. A ce titre, le fait qu'une *personne physique* interagisse avec un SIA peut la priver de ce droit d'avoir des relations avec d'autres êtres humains[60]. Une personne pourrait également être trompée, pensant interagir avec un être humain alors qu'elle est en relation avec un SIA. On peut citer l'exemple des *agents conversationnels (chatbot)* ou des *robots assistants*. En ce sens, l'AI Act prévoit une obligation d'information *by design* à la charge des fournisseurs

de certains SIA, en particulier ceux destinés à interagir avec des personnes physiques et ceux qui génèrent des contenus synthétiques (AI Act, art. 50,§§1 et 2 et cons. 132).

49. Deuxième facteur de risque : la vidéosurveillance. Les dispositifs de *vidéosurveillance*, qu'ils soient utilisés dans des lieux privés ou dans des lieux publics, comme la voie publique ou des locaux commerciaux ou des espaces de travail, présentent des risques importants d'atteinte au droit au respect de la vie privée.

50. Troisième facteur de risque : l'usage de SIA dans le domicile. Il peut aussi y avoir un risque d'atteinte à la vie privée lorsque le SIA est utilisé dans le *domicile* des personnes physiques ou morales. On peut notamment penser à la *domotique*. En effet, les informations collectées sur les utilisations du domicile de la personne peuvent révéler des informations sur sa vie privée, comme ses habitudes de vie ou ses relations personnelles.

51. Quatrième facteur de risque : l'usage des SIA dans le cadre des communications. L'usage d'un SIA pour analyser le contenu de *communications* ou pour produire des communications textuelles, visuelles ou orales pourrait porter atteinte à la vie privée. Il s'agit par exemple de SIA destinés à analyser les courriers électroniques afin de détecter si les courriers reçus sont des *spams* ou des communications commerciales, voire même pour des assistants de rédaction de messages.

52. Cinquième facteur de risque : l'identification biométrique à distance en temps réel. Les systèmes d'*identification biométrique à distance en temps réel* sont expressément désignés par l'AI Act comme porteurs de risque pour la protection de la liberté. Selon ce texte, il s'agit de systèmes dans lesquels l'acquisition des données biométriques, la comparaison et l'identification se déroulent sans décalage temporel significatif. Selon l'AI Act, l'utilisation de ces systèmes est particulièrement « intrusive pour les droits et les libertés des personnes concernées, dans la mesure où elle peut toucher la vie privée d'une grande partie de la population, susciter un sentiment de surveillance constante et dissuader indirectement l'exercice de la liberté de réunion et d'autres droits fondamentaux », notamment lorsqu'ils sont utilisés à des fins répressives (AI Act, cons. 32).

53. Sixième facteur de risque : la reconnaissance faciale. Selon l'AI Act, les systèmes de *reconnaissance faciale* peuvent accentuer le sentiment de surveillance de masse et entraîner des violations du droit au respect de la vie privée. C'est notamment le cas des SIA créant ou développant des bases de données de reconnaissance faciale par le moissonnage non ciblé d'images faciales provenant de l'internet ou de la vidéosurveillance, qui sont à ce titre interdits par l'AI Act (AI Act, art. 5 , §1, e) et cons. 43).

b. La protection des données à caractère personnel (art. 8 de la Charte)

CHARTE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE

ARTICLE 8 - PROTECTION DES DONNEES A CARACTERE PERSONNEL

1. TOUTE PERSONNE A DROIT A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL LA CONCERNANT.

2. CES DONNEES DOIVENT ETRE TRAITEES LOYALEMENT, A DES FINS DETERMINEES ET SUR LA BASE DU CONSENTEMENT DE LA PERSONNE CONCERNEE OU EN VERTU D'UN AUTRE FONDEMENT LEGITIME PREVU PAR LA LOI. TOUTE PERSONNE A LE DROIT D'ACCEDER AUX DONNEES COLLECTEES LA CONCERNANT ET D'EN OBTENIR LA RECTIFICATION.

3. LE RESPECT DE CES REGLES EST SOUMIS AU CONTROLE D'UNE AUTORITE INDEPENDANTE.

i. Le cadre juridique

54. Les rapports entre les articles 7 et 8 de la Charte. Il apparaît que le champ d'application du droit au respect de la vie privée et familiale garanti par l'article 7 de la Charte recoupe dans de nombreux domaines la protection des données à caractère personnel régie par l'article 8 de la Charte. Il en est ainsi de la protection des prénom et nom de la personne, qui sont également des données à caractère personnel au sens de l'article 4 du RGPD[61]. En pratique, la CJUE a « appliqué ces dispositions de concert dans de nombreux arrêts, considérant notamment que le traitement de données personnelles (accès, utilisation, conservation, communication...) constitue de manière cumulative une atteinte distincte aux articles 7 et 8 de la Charte »[62].

La consécration de la protection des données à caractère personnel dans la Charte reflète l'importance du traitement de ces données dans nos sociétés, rendant nécessaire une protection spécifique distincte de la protection de la vie privée afin de développer un régime propre de la protection des données répondant aux enjeux particuliers du traitement des données à caractère personnel et de « déterminer le plus finement possible dans quelle mesure les données personnelles des individus peuvent faire l'objet d'un traitement sans porter atteinte à leurs droits »[63].

En revanche, il est possible de dissocier strictement la protection de la vie privée et la protection des données à caractère personnel en matière de communications des personnes morales puisque la protection des données à caractère personnel ne concerne que les personnes physiques et non pas les personnes morales[64].

55. Le cadre législatif européen : le règlement 2016/679 (RGPD), la directive 2016/680 et le règlement 2018/1725. La protection des données à caractère personnel se fonde principalement sur le règlement 2016/679 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 dit règlement général sur la protection des données (ci-après RGPD). Ce règlement définit les droits des personnes concernées et les obligations des responsables de traitements.

Il faut noter que l'Union européenne a adopté un instrument spécifique pour le traitement des données par les autorités publiques à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales. Il s'agit de la directive 2016/680 du 27 avril 2016. Cette directive contient des dispositions similaires, voire identiques, à celles du RGPD mais vise spécifiquement les autorités publiques compétentes en matière pénale ou de sécurité publique tandis que le RGPD concerne tout « traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier »[65].

Il existe également un texte visant spécifiquement le traitement des données à caractère personnel par les institutions, organes et organismes de l'Union reprenant les principes fondamentaux du RGPD. Il s'agit du règlement 2018/1725 du 23 octobre 2018.

56. Les notions de « donnée à caractère personnel » et de « traitement de données à caractère personnel ». Les notions essentielles du RGPD sont celles de « donnée à caractère personnel » et de « traitement de données à caractère personnel ».

Les données à caractère personnel sont définies par l'article 4, 1 du RGPD comme « toute information se rapportant à une personne physique identifiée ou identifiable », dénommée « personne concernée ». Une « personne physique identifiée ou identifiable » est « une personne physique une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ». La notion de donnée à caractère personnel est large et englobe toutes sortes de données. Ainsi, les nom et prénom d'une personne[66], son adresse postale[67], électronique[68] ou IP[69], son numéro de sécurité sociale[70] ou encore son image, sa voix, ses empreintes digitales, sa démarche ou son ADN[71] sont considérées comme des données à caractère personnel. Mais plus largement, la notion de donnée à caractère personnel « englobe les informations touchant à la vie privée et familiale d'une personne physique, *stricto sensu*, mais également les informations relatives à ses activités, quelles qu'elles soient, tout comme celles concernant ses relations de travail ainsi que son comportement économique ou social. Il s'agit donc d'informations concernant des personnes physiques, indépendamment de leur situation ou de leur qualité (en tant que consommateurs, patients, employés, clients, etc.) »[72]. Par exemple, « les titres de livres achetés par une personne sur une librairie en ligne ou les chansons écoutées via un service de diffusion en flux de musique »[73] sont considérées comme des données à caractère personnel.

Parmi les données à caractère personnel, il faut distinguer certaines catégories de données, dites « sensibles » dont le traitement est en principe interdit selon l'article 9 de RGPD. Cet article prohibe « le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ».

Concernant cette notion de traitement, il s'agit, d'après l'article 4, 2 du RGPD, de « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».

57. La protection des données à caractère personnel : l'articulation entre l'étude d'impact sur les VUE et l'analyse d'impact sur la protection des données. Le régime du traitement de données à caractère personnel présente deux volets. D'une part, le RGPD accorde des droits aux individus opposables aux responsables de traitement[74] et, d'autre part, le RGPD impose des obligations aux responsables de traitement[75].

Ce guide pratique n'a pas vocation à développer le régime de protection des données à caractère personnel. Néanmoins, dans la mesure où une violation du RGPD est susceptible de porter atteinte au droit fondamental de la protection des données à caractère personnel et à

la valeur « liberté », il convient de prendre en compte le risque d'atteinte au droit à la protection des données à caractère personnel.

L'analyse et le traitement de ces risques doit s'appuyer sur les dispositions du RGPD. En effet, l'AI Act précise que les fournisseurs et les déployeurs de SIA, en leur qualité de responsables de traitement et de sous-traitants, sont tenus de respecter le RGPD (AI Act, cons. 10). Concernant leurs qualifications respectives au regard du RGPD, il semble possible de considérer que le déployeur sera généralement le responsable du traitement tandis que le fournisseur pourrait être un sous-traitant s'il traite des données à caractère personnel pour le compte du déployeur[76]. Néanmoins, le fournisseur peut également être qualifié de responsable de traitement. D'après la Cnil, « un fournisseur qui est à l'initiative du développement d'un système d'IA et qui constitue la base de données d'apprentissage de son système d'IA à partir de données qu'il a sélectionnées lui-même pour son propre compte, peut être qualifié de responsable de traitement ». Par exemple, « le fournisseur d'un agent conversationnel qui entraîne son modèle de langage (« *Large Language Model* » ou LLM en anglais) à partir de données publiquement accessibles sur Internet, est responsable de traitement de la réutilisation des données personnelles publiquement accessibles sur Internet. En effet, il décide à la fois de l'objectif (entraîner un système d'IA) et des moyens essentiels du traitement (sélectionner les données qu'il va réutiliser) »[77]. La qualification du fournisseur est donc variable et il convient, à chaque étape du cycle de vie du SIA, de la redéfinir spécifiquement.

L'analyse et le traitement des risques pour la protection des données à caractère personnel peut nécessiter de réaliser une analyse d'impact sur la protection des données (AIPD)[78], seule à même d'identifier ces risques et de prendre les mesures adéquates pour les réduire. L'analyse d'impact sur la protection des données doit obligatoirement être réalisée par le responsable du traitement lorsque le traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques »[79]. Le Comité européen à la protection des données présume que le responsable du traitement est tenu de réaliser une analyse d'impact lorsque deux des neufs critères suivants sont remplis :

- l'évaluation ou notation des personnes ;
- la prise de décisions automatisée avec effet juridique ou effet similaire significatif ;
- la surveillance systématique ;
- le traitements de données sensibles ou à caractère hautement personnel ;
- le traitement de données à grande échelle ;
- la collecte de données de personnes vulnérables, comme par exemple les personnes mineures ;
- le croisement ou la combinaison d'ensembles de données ;
- l'utilisation innovante ou l'application de nouvelles solutions technologiques ou organisationnelles[80].

La Cnil estime que « dans tous les cas, il convient de s'interroger sur l'existence de risques pour les personnes du fait de la constitution d'une base d'entraînement et de son utilisation : si des risques importants existent, notamment du fait d'un mésusage des données, d'une violation de données, ou lorsque le traitement peut donner lieu à une discrimination, une AIPD doit être réalisée même si deux de ces critères ne sont pas remplis ; à l'inverse, une AIPD n'a pas à être réalisée si deux critères sont remplis mais que le responsable de traitement peut

établir de façon suffisamment certaine que le traitement des données personnelles en cause n'expose pas les individus à des risques élevés »[81].

Selon la Cnil, l'usage d'un SIA « ne relève pas systématiquement de l'usage innovant ou de l'application de nouvelles solutions technologiques ou organisationnelles. Tout traitement utilisant un système d'IA ne remplira donc pas ce critère. Afin de déterminer si la technique utilisée relève de tels usages, il conviendra de distinguer deux catégories de systèmes :

- Les systèmes qui utilisent des techniques d'IA validées expérimentalement depuis plusieurs années et éprouvées en conditions réelles ne relèvent pas de l'usage innovant ou de l'application de nouvelles solutions technologiques ou organisationnelles. […]
- Les systèmes qui utilisent des techniques encore nouvelles, notamment celles reposant sur des approches statistiques telles que l'apprentissage profond et dont les risques commencent juste à être connus aujourd'hui et sont encore mal maitrisés relèvent de l'usage innovant »[82].

La Cnil a également précisé que « si le développement d'un système d'IA repose souvent sur le traitement d'une grande quantité de données, cela ne relève pas nécessairement du traitement à grande échelle qui vise à « traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational [et qui peut] affecter un nombre important de personnes concernées » (considérant 91 du RGPD). Pour les systèmes d'IA, il conviendra notamment de déterminer si le développement concerne un très grand nombre de personnes »[83]. Le CEPD recommande de prendre en compte les facteurs suivants : le nombre de personnes concernées, soit en valeur absolue, soit en proportion de la population considérée ; le volume de données et/ou l'éventail des différents éléments de données traitées ; la durée ou la permanence de l'activité de traitement de données ; l'étendue géographique de l'activité de traitement[84].

Enfin, se pose la question du périmètre de l'analyse d'impact. La Cnil estime que « le périmètre de l'AIPD peut différer en fonction de la connaissance que le fournisseur a de l'usage qui sera fait, par lui-même ou par [le déployeur], du système d'IA qu'il développe ». La Cnil distingue deux situations :

- Le cas où l'usage opérationnel du système d'IA en phase de déploiement est identifié dès la phase de développement

  Deux hypothèses doivent être distinguées :
  - « Lorsque le fournisseur du système est également responsable du traitement pour la phase de déploiement et que l'usage opérationnel du système d'IA en phase de déploiement est identifié dès la phase de développement, il est recommandé de réaliser une AIPD générale pour l'ensemble du traitement. Le fournisseur pourra alors compléter cette AIPD par les risques liés aux deux phases. »
  - « Si le fournisseur n'est pas responsable du traitement pour la phase de déploiement mais qu'il identifie les finalités d'usage en phase de déploiement, il peut proposer au responsable du traitement un modèle d'AIPD. Cela peut lui permettre notamment de tenir compte de certains risques qu'il est plus facile d'identifier lors de la phase de développement.

Toutefois, [le déployeur], en tant que responsable de traitement, reste tenu de réaliser une AIPD, par exemple sur la base du modèle du fournisseur, s'il le souhaite. »

- Le cas où l'usage opérationnel du système d'IA en phase de déploiement n'est pas clairement identifié dès la phase de développement

« Dans cette hypothèse, le fournisseur ne pourra réaliser son analyse d'impact que sur la phase de développement. Il appartiendra ensuite au responsable du traitement de la phase de déploiement d'analyser, au regard des caractéristiques du traitement, si une AIPD est nécessaire pour cette phase. Le cas échéant, si les finalités de la phase de déploiement sont multiples, le responsable de traitement pourra décliner une même AIPD générale pour chacun des cas d'usages spécifiques. »[85]

S'il est obligatoire de réaliser une analyse d'impact sur la protection des données, cette analyse d'impact pourra être intégrée à la présente étude d'impact sur les VUE et leurs droits et principes fondamentaux de concrétisation. Par analogie, l'AI Act va en sens s'agissant de l'analyse d'impact sur les droits fondamentaux prévue pour certains déployeurs de SIA à haut risque selon l'article 27, 4 de l'AI Act.

ii. Les risques d'atteinte par les SIA

58. Les risques pour la protection des données et les SIA. Le traitement de *données à caractère personnel* par un SIA implique de nombreux risques pour le droit à la protection des données à caractère personnel. Cette problématique se pose dès lors que le SIA traite des données relatives à des *personnes physiques*.

La Cnil a identifié les risques spécifiques suivants pour les traitements de données reposant sur des SIA :

- « les risques pour les personnes concernées liés à des mésusages des données contenues dans la base d'apprentissage, notamment en cas de violation de données ;
- le risque d'une discrimination automatisée causée par un biais du système d'IA introduit lors du développement et causant une performance moindre du système pour certaines catégories de personnes ;
- le risque de produire du contenu fictif erroné sur une personne réelle, particulièrement important dans le cas des systèmes d'IA génératives, et pouvant avoir des conséquences sur sa réputation ;
- le risque de prise de décision automatisée causée par un biais d'automatisation ou de confirmation dans le cas où les mesures d'explicabilité nécessaires ne sont pas prises lors du développement de la solution (comme la remontée d'un score de confiance, ou d'informations intermédiaires tel qu'une carte de saillance ou « *saliency map* ») ou si un agent utilisant le système d'IA ne peut pas prendre une décision contraire sans que cela ne lui porte préjudice ;
- le risque d'une perte de contrôle des utilisateurs sur leurs données publiées et librement accessibles en ligne, une collecte à large échelle étant souvent nécessaire à l'apprentissage d'un système d'IA, notamment lorsque celles-ci sont collectées par moissonnage ou « *webscraping* » ;

- les risques liés aux attaques connues spécifiques aux systèmes d'IA tel que les attaques par empoisonnement des données, par insertion d'une porte dérobée, ou encore par inversion du modèle ;
- les risques liés à la confidentialité des données susceptibles d'être extraites depuis le système d'IA »[86].

A l'aune de l'AI Act, l'ensemble des cas d'usage de SIA à haut risque ou soumis à des obligations de transparence sont potentiellement concernés par ces risques. Sont probablement plus exposés les SIA dont le fonctionnement repose à titre principal sur le traitement de données personnelles sensibles[87] à l'instar des SIA en matière de biométrie (annexe III, §1).

[43] MOLINIER Joël (dir.), *Les principes fondateurs de l'Union européenne*, Paris : Puf, coll. Droit et justice, 2005, p. 159

[44] MOLINIER Joël, « Principes généraux – Teneur des principes généraux du droit », *Répertoire de droit européen*, 2011, n° 70

[45] Conseil de l'Europe, *Guide sur l'article 8 de la Convention européenne des droits de l'homme Droit au respect de la vie privée et familiale, du domicile et de la correspondance*, 2022, p. 26 ; CEDH, 14 mai 2002, Zehnalová et Zehnal c/ République tchèque, req. n° 38621/97

[46] CARIAT Nicolas, « Article 7 Respect de la vie privée et familiale », *In* PICOD Fabrice et RIZCALLAH Cecilia et VAN DROOGHENBROECK Sébastien (dir.), *Charte des droits fondamentaux de l'Union européenne : Commentaire article par article*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 3ème éd., 2023, p. 177

[47] CJCE, 14 février 2008, Varec, aff. C-450/0

[48] CJUE, 9 nov. 2010,Volker, aff. jtes C-92/09 et C-93/09

[49] CJUE, 8 déc. 2022, Google LLC, aff. C-460/20

[50] CJUE, 12 mai 2011, Runevič-Vardyn et Wardyn, aff. C-391/09 ; CJUE, 22 déc. 2010, Sayn-Wittgenstein, aff. C-208/09

[51] CJUE, 5 juin 2018, Coman, aff. C-673/16

[52] CJUE, 4 avril 2019, OZ c. BEI, aff. C-558/17 P

[53] TPICE, 28 janv. 2005, Evonik Degussa c/ Commission, aff. t-341/12

[54] CJUE, 11 déc. 2019, TK c/ Asociaţia de Proprietari bloc M5A-ScaraA, aff. C-708/18

[55] CJUE, 18 juin 2015, Deutsche Bahn AG c/ Commission, aff. C-583/13 P

[56] V. BUFFELAN-LANORE Yvaine, « Domicile, demeure et logement familial – Caractères du domicile », *Répertoire de droit civil*, 2014, chap. 3 sect. 2

[57] CJCE, 22 oct. 2002, Roquette Frères c/ Directeur général de la concurrence, de la consommation et de la répression des fraudes, aff. C-94/00, §29

[58] CJUE, 17 décembre 2015, WebMindLicenses, aff. C-419/14, pt. 71 et 72

[59] CARIAT Nicolas, « Article 7 Respect de la vie privée et familiale », *In* PICOD Fabrice et RIZCALLAH Cecilia et VAN DROOGHENBROECK Sébastien (dir.), *Charte des droits fondamentaux de l'Union européenne : Commentaire article par article*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 3ème éd., 2023, p. 177

[60] MEYER-HEINE Anne, « Robots, personnes âgées et droit de l'Union européenne », Revue de l'Union européenne, 2019, p. 246

[61] RGPD, art. 4, 1 : « données à caractère personnel », toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom […] ».

[62] CARIAT Nicolas, « Article 7 Respect de la vie privée et familiale », *In* PICOD Fabrice et RIZCALLAH Cecilia et VAN DROOGHENBROECK Sébastien (dir.), *Charte des droits fondamentaux de l'Union européenne : Commentaire article par article*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 3ème éd., 2023, p. 184 ; v. CJUE, 8 avril 2014, Digital Rights Ireland et Seitlinger *et al*., aff. C-293/12 et CJUE, 16 juill. 2020, Facebook Ireland et Schrems, aff. C-311/18

[63] TINIERE Romain, « Article 8 Protection des données à caractère personnel » , *In* PICOD Fabrice et RIZCALLAH Cecilia et VAN DROOGHENBROECK Sébastien (dir.), *Charte des droits fondamentaux de*

l'Union européenne : Commentaire article par article, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 3ème éd., 2023, p. 209

[64] TINIERE Romain et VIAL Claire, *Droit de l'Union européenne des droits fondamentaux*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 2023Manuel de droit de l'Union européenne des droits fondamentaux, p. 415

[65] RGPD, art. 2

[66] RGPD, art. 4, 1 : « nom »

[67] RGPD, art. 4, 1 : « données de localisation »

[68] RGPD, art. 4, 1 : « identifiant en ligne »

[69] CJUE 24 nov. 2011, Sté Scarlet Extended c/ Société belge des auteurs, compositeurs et éditeur SCRL, aff. C-70/10

[70] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 30

[71] G29, *Avis 4/2007 sur le concept de données à caractère personnel*, 20 juin 2007, WP 136, p. 9

[72] G29, *Avis 4/2007 sur le concept de données à caractère personnel*, 20 juin 2007, WP 136, p. 7

[73] G29, *Lignes directrices relatives au droit à la portabilité des données*, 5 avril 2017, WP 242 rev.01

[74] Les personnes concernées ont le droit d'obtenir une information transparente sur le traitement des données les concernant (RGPD, art. 12, 13, 14 et 19), d'accéder aux données (RGPD, art. 15), d'obtenir la rectification des données inexactes et incomplètes (RGPD, art. 16), d'obtenir l'effacement des données (un « droit à l'oubli ») (RGPD, art. 17), d'obtenir la limitation du traitement (RGPD, art. 18), à la portabilité des données (RGPD, art. 20), d'opposition au traitement (RGPD, art. 21) et « 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 » (RGPD, art. 22).

[75] Le responsable du traitement doit respecter les principes relatifs aux traitements de données à caractère personnel énoncés par l'article 5 de RGPD (licéité, loyauté et transparence ; limitation des finalités ; minimisation des données ; exactitude ; limitation de la conservation ; intégrité et confidentialité ; et responsabilité ou *accountability*).

Concernant spécifiquement le principe de licéité, le responsable du traitement doit fonder son traitement sur l'une des bases légales de l'article 6 du RGPD (consentement des personnes concernées ; exécution d'un contrat ; respect d'une obligation légale ; sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ; exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ; intérêts légitimes poursuivis par le responsable du traitement ou par un tiers).

Puis le responsable du traitement a l'obligation de garantir la protection des données dès la conception (*by design*) et par défaut (*by default*) (RGPD, art. 25). Cette protection des données s'entend de la garantie du droit à la protection des données au sens large et non pas de la seule sécurité des données, qui constitue une obligation particulière à la charge du responsable du traitement (RGPD, art. 32, 33 et 34).

Le responsable du traitement doit également tenir un registre des opérations de traitement (RGPD, art. 30), coopérer avec l'autorité de contrôle (RGPD, art. 31), et, dans certains conditions, réaliser une analyse d'impact relative à la protection des données (RGPD, art. 35) pouvant aboutir à une obligation de consultation préalable de l'autorité de contrôle (RGPD, art. 36). Il peut en outre dans certains cas être obligé de désigner un délégué à la protection des données (RGPD, art. 37).

[76] Le responsable du traitement est selon l'article 4, 7 du RGPD « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ». Le déployeur étant la personne qui utilise sous sa propre autorité un SIA, il est possible de considérer que le terme d' « autorité » couvre la détermination des finalités et des moyens du traitement de données à caractère personnel. Le fournisseur pourrait quant à lui être considéré comme un sous-traitant. Le sous-traitant est selon l'article 4, 8 du RGPD « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ». Selon la Cnil, un « fournisseur de système d'IA peut […] être sous-traitant lorsque qu'il développe un système d'IA pour le compte d'un de ses clients, dans le cadre d'une prestation. Le client est pour sa part responsable de traitement dès lors qu'il détermine la finalité et les moyens du traitement ». Elle précise cependant que « dans d'autres configurations, le fournisseur de système d'IA peut être responsable de traitement des systèmes qu'il conçoit pour les commercialiser » [Cnil, « Déterminer la qualification juridique des fournisseurs de systèmes d'IA », *Cnil.fr* [en ligne], 11 oct. 2023. Disponible sur : https://www.cnil.fr/fr/determiner-la-qualification-juridique-des-fournisseurs-de-systemes-dia]

[77] Cnil, « Déterminer la qualification juridique des fournisseurs de systèmes d'IA », *Cnil.fr* [en ligne], 11 oct. 2023. Disponible sur : https://www.cnil.fr/fr/determiner-la-qualification-juridique-des-fournisseurs-de-systemes-dia

[78] RGPD, art. 35 et 36

[79] RGPD, art. 35

[80] Pour plus de détails, v. CEPD, *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*, 4 oct. 2017, WP 248 rév. 01, nota. p. 9 et s.

[81] Cnil, « Réaliser une analyse d'impact si nécessaire », *Cnil.fr* [en ligne], 11 oct. 2023. Disponible sur : https://www.cnil.fr/fr/realiser-une-analyse-dimpact-si-necessaire-0

[82] Cnil, « Réaliser une analyse d'impact si nécessaire », *Cnil.fr* [en ligne], 11 oct. 2023. Disponible sur : https://www.cnil.fr/fr/realiser-une-analyse-dimpact-si-necessaire-0

[83] Cnil, « Réaliser une analyse d'impact si nécessaire », *Cnil.fr* [en ligne], 11 oct. 2023. Disponible sur : https://www.cnil.fr/fr/realiser-une-analyse-dimpact-si-necessaire-0

[84] CEPD, *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*, 4 oct. 2017, WP 248 rév. 01, p. 12

[85] Cnil, « Réaliser une analyse d'impact si nécessaire », *Cnil.fr* [en ligne], 11 oct. 2023. Disponible sur : https://www.cnil.fr/fr/realiser-une-analyse-dimpact-si-necessaire-0

[86] Cnil, « Réaliser une analyse d'impact si nécessaire », *Cnil.fr* [en ligne], 11 oct. 2023. Disponible sur : https://www.cnil.fr/fr/realiser-une-analyse-dimpact-si-necessaire-0

[87] RGPD, cons. 10 et art. 9. Il s'agit du traitement de données « qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ». Le traitement de ces données est en principe interdit et n'est autorisé que dans les conditions énoncées au paragraphe 2 de l'article 9 (par ex. si la personne concernée a donné son consentement explicite à moins que le droit de l'Union ou de l'État membre interdise de lever cette prohibition par consentement).

3. L'égalité

59. La notion d'égalité. La notion d' « égalité » a différentes acceptions. En premier lieu, l'égalité peut être considérée comme un égalité « formelle » ou « constitutionnelle » consistant à une égalité devant la loi[88]. L'article 20 de la Charte indique ainsi que « toutes les personnes sont égales en droit ». Ce principe signifie que le droit ne doit pas intégrer de distinctions injustifiées entre les citoyens, notamment des distinctions fondées sur la race ou la religion. Par exemple, l'article 2, 1 de la 2000/43/CE du 29 juin 2000 relative à la mise en œuvre du principe de l'égalité de traitement entre les personnes sans distinction de race ou d'origine ethnique définit l'égalité de traitement comme « l'absence de toute discrimination directe ou indirecte fondée sur la race ou l'origine ethnique »[89].

En second lieu, l'égalité renvoie à l'idée de non-discrimination[90]. Il s'agit d'un principe fondamental du droit de l'Union européen selon lequel des situations comparables ne doivent pas être traitées de manière différente à moins qu'une différenciation ne soit objectivement justifiée mais aussi que des mêmes règles ne doivent pas être appliquées à des situations différentes[91].

60. Les droits et principes fondamentaux de concrétisation. L'égalité, en tant que VUE, est concrétisée par divers droits et principes fondamentaux. En contexte IA, les droits les plus susceptibles d'être affectés sont le droit à la non-discrimination (a), les droits de l'enfant (b) et le droit d'intégration des personnes handicapées (c).

a. Le droit à la non-discrimination (art. 21 de la Charte)

CHARTE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE
ARTICLE 21 - NON-DISCRIMINATION
1. EST INTERDITE TOUTE DISCRIMINATION FONDEE NOTAMMENT SUR LE SEXE, LA RACE, LA COULEUR, LES ORIGINES ETHNIQUES OU SOCIALES, LES CARACTERISTIQUES GENETIQUES, LA LANGUE, LA RELIGION OU LES CONVICTIONS, LES OPINIONS POLITIQUES OU TOUTE AUTRE OPINION, L'APPARTENANCE A UNE MINORITE NATIONALE, LA FORTUNE, LA NAISSANCE, UN HANDICAP, L'AGE OU L'ORIENTATION SEXUELLE.
2. DANS LE DOMAINE D'APPLICATION DES TRAITES ET SANS PREJUDICE DE LEURS DISPOSITIONS PARTICULIERES, TOUTE DISCRIMINATION EXERCEE EN RAISON DE LA NATIONALITE EST INTERDITE.

i. Le cadre juridique

61. Le principe d'égalité de traitement. Le principe de non-discrimination prend appui sur le principe d'égalité de traitement. Il ressort de la jurisprudence de la CJUE que « le principe d'égalité de traitement exige que des situations comparables ne soient pas traitées de manière différente et que des situations différentes ne soient pas traitées de manière égale, à moins qu'un tel traitement ne soit objectivement justifié »[92]. Ce principe implique donc, d'une part, de traiter de façon égale des individus placés dans les mêmes situations et, d'autre part, de traiter différemment des individus placés dans des situations différentes. On comprend donc que « différenciation et discrimination ne sont pas synonymes [..] dès lors que la discrimination

peut résulter d'une absence de différenciation »[93]. Une différence de traitement est justifiée, selon la CJUE, dès lors qu'elle est fondée sur un critère objectif et raisonnable, c'est-à-dire lorsqu'elle est en rapport avec un but légalement admissible, poursuivi par la législation en cause et que cette différence est proportionnée au but poursuivi par le traitement concerné[94].

62. L'articulation entre l'article 21 et les autres dispositions de la Charte. L'article 21 de la Charte constitue « une expression particulière du principe général d'égalité de traitement consacré à l'article 20 de la Charte »[95] énonçant que « toutes les personnes sont égales en droit ». L'article 21 précise les dispositions de l'article 20 « en instaurant une clause d'interdiction de discrimination fondée sur une liste actualisée et ouverte de motifs ».

L'article 21 doit également être lu en combinaison avec les autres articles du chapitre de la Charte consacré à l'égalité précisant les droits de certaines catégories de personnes, comme les articles 24 relatif aux droits de l'enfant[96] et 26 relatif au droit d'intégration des personnes handicapées[97].

63. Une liste ouverte. Le paragraphe 1 de l'article 21 de la Charte pose une liste de motifs de discrimination prohibés. Ces motifs sont les suivants : « le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge ou l'orientation sexuelle ». L'intérêt de cette liste consiste à rendre possible, d'une part, une action contre une discrimination qui ne serait pas expressément sanctionnée par une directive ou un règlement européen et, d'autre part, une action pour dénoncer une discrimination fondée sur plusieurs motifs, par exemple fondée sur le genre et l'orientation sexuelle[98].

Enfin, cette liste n'est pas limitative[99] ainsi que le révèle l'emploi de l'adverbe l'introduisant « notamment ». Ceci implique que des discriminations non précisées par le texte pourraient néanmoins être sanctionnées sur ce fondement, comme les discriminations intersectionnelles

64. Les discriminations fondées sur le sexe. Le paragraphe 2 de l'article 21 de la Charte prohibe en premier lieu les discriminations fondées sur le sexe, c'est-à-dire qu'il pose le principe de l'égalité des sexes. L'égalité des sexes se manifeste notamment en matière d'emploi[100], en matière économique[101] ou dans les fonctions occupées dans la vie politique et économique[102].

Selon le principe d'égalité des sexes, la prise en considération du sexe ne devrait avoir aucune conséquence positive ou négative sur les personnes. La prise en compte du sexe doit rester « neutre »[103]. Ce principe se décline notamment en principe de l'égalité des rémunérations[104]. Le principe d'égalité des sexes interdit les discriminations directes fondées sur le sexe, « y compris un traitement moins favorable de la femme en raison de la grossesse et de la maternité » ainsi que les discriminations indirectes[105]. La discrimination directe est définie comme « la situation dans laquelle une personne est traitée de manière moins favorable en raison de son sexe qu'une autre ne l'est, ne l'a été ou ne le serait dans une situation comparable ». Quant à la discrimination indirecte, elle vise « la situation dans laquelle une disposition, un critère ou une pratique apparemment neutre désavantagerait particulièrement des personnes d'un sexe par rapport à des personnes de l'autre sexe, à moins que cette disposition, ce critère ou cette pratique ne soit objectivement justifié par un but légitime et que les moyens pour parvenir à ce but ne soient appropriés et nécessaires »[106]. Ainsi, alors que la

discrimination directe ne peut pas être justifiée par un motif d'intérêt général, la discrimination indirecte peut l'être à l'issue d'un contrôle de proportionnalité[107].

En revanche, le principe d'égalité des sexes n'interdit pas des « discriminations positives » destinées à prévenir ou à compenser des désavantages liés au sexe[108], notamment dans les secteurs d'activité où les femmes sont moins nombreuses que les hommes au niveau du poste considéré dans certaines conditions[109].

L'égalité de traitement concerne également les questions relatives à l'identité sexuelle et à la transsexualité[110].

65. Les discriminations fondées sur la race, la couleur et les origines ethniques. Les discriminations fondées sur la race, la couleur de peau et les origines ethniques des personnes sont également interdites par la directive 2000/43/CE du 29 juin 2000 relative à la mise en œuvre du principe de l'égalité de traitement entre les personnes sans distinction de race ou d'origine ethnique. Ce texte reprend à son compte la distinction précitée entre discrimination directe et indirecte[111].

L'objectif de cette directive est de lutter contre les discriminations raciales et ethniques dans de multiples secteurs de la vie économique et de la politique sociale et éducative. Elle s'applique, entre autres, à l'accès à l'emploi, à la protection sociale et à l'éduction[112].

Enfin, la directive ne s'oppose pas aux politiques de « discrimination positive », appelées « action positive » dans ce texte[113].

66. Les discriminations fondées sur les caractéristiques génétiques. L'article 21 de la Charte prohibe les discrimination fondées sur les caractéristiques génétiques des personnes. Cette prohibition est susceptible d'être couplée avec l'interdiction des discriminations liées au handicap, par exemple dans le cas d'une maladie génétique source de handicap pour la personne atteinte, à l'instar de la trisomie 21.

L'interdiction des discriminations fondées sur les caractéristiques génétiques vise notamment à protéger les personnes contre les discriminations liées à leur état de santé actuel ou les projections relatives à cet état de santé au regard de leurs caractéristiques génétiques. En ce sens, l'article L. 225-3 du code pénal français, par exemple, sanctionne les discriminations fondées « sur la prise en compte de tests génétiques prédictifs ayant pour objet une maladie qui n'est pas encore déclarée ou une prédisposition génétique à une maladie ».

67. Les discriminations fondées sur la religion ou les convictions. L'article 21 de la Charte protège également les personnes contre les discriminations ayant pour origine leur religion ou leurs convictions philosophiques ou spirituelles[114]. En ce sens, la directive 2000/78/CE du 27 novembre 2000 portant création d'un cadre général en faveur de l'égalité de traitement en matière d'emploi et de travail[115] adopte, à nouveau ici, la distinction entre discrimination directe et indirecte. Ces discriminations concernent, par exemple, les mesures qui peuvent être prises par une personne publique ou privée visant les signes religieux[116].

68. Les discriminations fondées sur les opinions politiques ou toute autre opinion. La Charte protège, en outre, les personnes contre les discriminations fondées sur leurs opinions politiques ou toute autre opinion. La CJUE a eu notamment l'occasion de contrôler sur le fondement de la directive 2000/78/CE précitée les règles d'entreprise visant à instaurer une « neutralité politique »[117].

69. Les discriminations fondées sur le handicap. La protection des personnes handicapées contre les discriminations est également assurée par la directive 2000/78/CE.

Dans ce contexte, la CJUE distingue la notion de « handicap » de celle de « maladie ». En effet, selon la Cour, le législateur de l'Union ayant utilisé le terme de « handicap » dans la directive 2000/78, il « a délibérément choisi un terme qui diffère de celui de ‘‘maladie’’. Une assimilation pure et simple des deux notions est donc exclue »[118]. La CJUE définit la notion de « handicap » comme « visant une limitation, résultant notamment d'atteintes physiques, mentales ou psychiques et entravant la participation de la personne concernée à la vie professionnelle »[119]. Cette limitation doit être « de longue durée »[120]. L'obésité, par exemple, peut être considérée comme un handicap « notamment, si l'obésité du travailleur fait obstacle à sa pleine et effective participation à la vie professionnelle sur la base de l'égalité avec les autres travailleurs du fait d'une mobilité réduite ou de la survenance, chez cette personne, de pathologies qui l'empêchent d'accomplir son travail ou qui entraînent une gêne dans l'exercice de son activité professionnelle »[121].

La protection contre la discrimination vise les personnes handicapées et leur entourage[122].

Le principe d'égalité de traitement n'implique néanmoins pas une interdiction absolue de traiter différemment les personnes handicapées, dès lors qu'il est possible de constater une différence de situation entre les personnes handicapées et les autres personnes. Par exemple, la CJUE a considéré « [qu']une différence de traitement opérée sur une personne selon qu'elle possède ou non l'acuité visuelle nécessaire pour la conduite des véhicules à moteur n'est pas, en principe, contraire à l'interdiction de discrimination fondée sur le handicap au sens de l'article 21, paragraphe 1, de la Charte, pour autant qu'une telle exigence réponde effectivement à un objectif d'intérêt général, qu'elle soit nécessaire et qu'elle ne constitue pas une charge démesurée »[123].

70. Les discriminations fondées sur l'âge. La directive 2000/78 du 27 novembre 2000 précitée indique que les discriminations directes et indirectes fondées sur l'âge sont interdites. Elle précise également le cadre des différences de traitement fondées sur l'âge acceptables. Son article 6 indique qu'il est possible de prévoir des différences de traitement fondées sur l'âge « lorsqu'elles sont objectivement et raisonnablement justifiées, dans le cadre du droit national, par un objectif légitime, notamment par des objectifs légitimes de politique de l'emploi, du marché du travail et de la formation professionnelle, et que les moyens de réaliser cet objectif sont appropriés et nécessaires ».

71. Les discriminations fondées sur l'orientation sexuelle. La CJUE a développé sa jurisprudence relative aux discriminations fondées sur l'orientation sexuelle, en particulier l'homosexualité, dans le domaine de la politique sociale et de l'emploi. Par exemple, la Cour a considéré que le refus d'octroyer une pension de survie au conjoint survivant après le décès de l'affilié auquel il était lié par un « partenariat de vie »[124] au motif que l'intéressé n'était pas marié au défunt était un traitement moins favorable constitutif d'une discrimination fondée sur l'orientation sexuelle, les partenaires étant légalement dans l'impossibilité de se marier compte tenu de leur orientation sexuelle (selon le droit applicable dans l'État membre dans lequel vivait le couple, en l'occurrence en Allemagne) et alors que le droit national applicable (le droit allemand en l'occurrence) reconnaissait l'institution du « partenariat de vie », créant des droits et responsabilités identiques à la charge des intéressés que ceux existants entre époux[125].

A également été considéré comme constituant une discrimination fondée sur le sexe un arrêté national excluant de façon permanente du don du sang les hommes ayant eu des rapports sexuels avec d'autres hommes, puisqu'il subissait de la sorte un traitement moins favorable que les personnes hétérosexuelles masculines[126].

72. La nationalité : le paragraphe 2 de l'article 21 de la Charte. Le paragraphe 2 de l'article 21 de la Charte réserve une place particulière aux discriminations fondées sur la nationalité. Cela ressort également des actes législatifs de l'Union, à l'instar de la directive 2000/43/CE du 29 juin 2000 relative à la mise en œuvre du principe de l'égalité de traitement entre les personnes sans distinction de race ou d'origine ethnique, qui ne régissent pas « les différences de traitement fondées sur la nationalité »[127]. En effet, le principe de non-discrimination à raison de la nationalité est une règle cardinale et structurante en droit de l'Union qui découle, d'une part, des libertés de circulation du marché intérieur et, d'autre part, à titre subsidiaire, de la clause horizontale de l'article 18 du TFUE.

Néanmoins, malgré l'importance de ce principe, le paragraphe 2 de l'article 21 de la Charte, qui reprend les termes de l'article 18, alinéa 1er du TFUE[128], s'applique de façon subsidiaire[129]. Cela signifie que ce texte ne s'applique que dans les situations où les traités ne prévoient pas de règles spécifiques de non-discrimination qui pourraient être invoquées[130].

ii. Les risques d'atteinte par les SIA

73. Premier facteur de risque : la catégorisation biométrique. La *catégorisation biométrique* est « le classement de personnes physiques dans certaines catégories sur la base de leurs données biométriques. Ces catégories spécifiques peuvent concerner des aspects tels que le sexe, l'âge, la couleur des cheveux, la couleur des yeux, les tatouages, les traits liés au comportement ou à la personnalité, la langue, la religion, l'appartenance à une minorité nationale ou encore l'orientation sexuelle ou politique » (AI Act, cons. 16)[131]. L'AI Act précise que ces SIA peuvent conduire à des résultats biaisés et entraîner des effets discriminatoires. Le risque de tels résultats biaisés et d'effets discriminatoires est particulièrement important en ce qui concerne l'*âge*, l'*appartenance ethnique*, la *race*, la *couleur de peau*, le *sexe* ou le *handicap*. Ainsi, il y a risque important lorsqu'un SIA traite précisément ce type d'informations mais aussi des informations relatives aux *caractéristiques génétiques* de la personne, à sa *corpulence*, sa *démarche* ou encore sa *tenue vestimentaire*.

La catégorisation biométrique réalisée par un SIA peut s'avérer particulièrement problématique lorsqu'elle risque de priver une personne de certains droits et/ou de donner lieu à un traitement différent de cette personne par rapport à d'autres catégories d'individus, par exemple en matière d'*accès aux services publics* ou dans le secteur des *assurances*.

74. Deuxième facteur de risque : l'utilisation d'un SIA dans le cadre d'une relation de travail. L'utilisation de SIA dans le cadre d'une relation de *travail* fait naître des risques de discrimination. Comme l'indique l'AI act, « tout au long du processus de recrutement et lors de l'évaluation, de la promotion ou du maintien des personnes dans des relations professionnelles contractuelles, les systèmes d'IA peuvent perpétuer des schémas historiques de discrimination, par exemple à l'égard des femmes, de certains groupes d'âge et des personnes handicapées, ou de certaines personnes en raison de leur origine raciale ou ethnique ou de leur *orientation sexuelle* » (AI Act, cons. 56).

75. Troisième facteur de risque : l'utilisation d'un SIA dans le cadre de l'éducation et à la formation. L'utilisation de SIA dans le cadre de *l'éducation et de la formation* est selon l'AI Act à haut risque dans la mesure où des schémas discriminatoires visant certaines catégories de personnes peuvent être reproduits par le SIA et porter atteinte aux droits des personnes d'avoir accès à l'éducation et à la formation (AI Act, cons. 56 et annexe III, pt. 3).

Cela concerne l'utilisation du SIA pour déterminer l'accès ou l'admission aux établissements d'éducation et de formation, pour affecter des personnes à des établissements ou programmes d'enseignement et de formation professionnelle à tous les niveaux, pour évaluer les acquis d'apprentissage des personnes, pour évaluer le niveau d'enseignement approprié d'une personne et influencer substantiellement le niveau d'enseignement et de formation dont bénéficiera cette personne ou auquel elle pourra avoir accès ou pour surveiller les étudiants au cours des épreuves et détecter les comportements interdits.

b. Les droits de l'enfant (art. 24 de la Charte)

> *CHARTE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE*
> *ARTICLE 24 - DROITS DE L'ENFANT*
> *1. LES ENFANTS ONT DROIT A LA PROTECTION ET AUX SOINS NECESSAIRES A LEUR BIEN-ETRE. ILS PEUVENT EXPRIMER LEUR OPINION LIBREMENT. CELLE-CI EST PRISE EN CONSIDERATION POUR LES SUJETS QUI LES CONCERNENT, EN FONCTION DE LEUR AGE ET DE LEUR MATURITE.*
> *2. DANS TOUS LES ACTES RELATIFS AUX ENFANTS, QU'ILS SOIENT ACCOMPLIS PAR DES AUTORITES PUBLIQUES OU DES INSTITUTIONS PRIVEES, L'INTERET SUPERIEUR DE L'ENFANT DOIT ETRE UNE CONSIDERATION PRIMORDIALE.*
> *3. TOUT ENFANT A LE DROIT D'ENTRETENIR REGULIEREMENT DES RELATIONS PERSONNELLES ET DES CONTACTS DIRECTS AVEC SES DEUX PARENTS, SAUF SI CELA EST CONTRAIRE A SON INTERET.*

i. Le cadre juridique

76. Une protection spécifique des enfants. L'article 24 de la Charte, prenant compte de la vulnérabilité liée à l'âge et aux besoins particuliers des enfants, leur offre une protection spécifique. L'objectif de cet article est d'assurer le bien-être physique et moral de l'enfant.

C'est dans cette perspective de protection qu'a notamment été adoptée la directive 2011/93 du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie[132] dans l'espace judiciaire européen. Ce texte établit des règles minimales relatives à la définition des infractions pénales et des sanctions en matière d'abus sexuels perpétrés contre des enfants.

77. Les droits reconnus aux enfants. L'article 24 de la Charte reconnaît plusieurs droits aux enfants. En premier lieu, il leur accorde le droit d'exprimer librement leurs opinions. Ces opinions doivent être prises en considération pour les sujets qui les concernent, en fonction de leur âge et de leur maturité. En second lieu, les enfants ont le droit d'entretenir régulièrement des relations personnelles et des contacts directs avec leurs deux parents, sauf si cela est contraire à leur intérêt.

78. La primauté de l'intérêt supérieur de l'enfant. Le paragraphe 2 de l'article 24 de la Charte consacre la primauté de l'intérêt supérieur de l'enfant, qui sont des personnes âgées de moins de 18 ans, énonçant que « dans tous les actes relatifs aux enfants, qu'ils soient accomplis par des autorités publiques ou des institutions privées, l'intérêt supérieur de l'enfant doit être une considération primordiale ». La primauté de l'intérêt supérieur de l'enfant est également un élément central de la Convention des Nations Unies relative aux droits de l'enfant du 20 novembre 1989 qui a été ratifiée par l'ensemble des États membres de l'Union européenne et dans le monde entier, seuls les États-Unis, au sein des Nations Unies, n'ont pas ratifié cette convention[133].

Plusieurs textes de droit dérivé[134] et arrêts de la CJUE[135] consacrent la primauté de l'intérêt supérieur de l'enfant. Cette primauté implique que l'intérêt supérieur de l'enfant doit être pris en compte en premier lieu et principalement lors de l'adoption de toute mesure concernant un enfant[136]. Quant au contenu de l'intérêt supérieur de l'enfant, la directive 2011/93 précitée en matière d'infractions sexuelles contre des mineurs indique que lorsque les États membres apprécient l'intérêt supérieur de l'enfant, ils devraient « en particulier tenir dûment compte du principe de l'unité familiale, du bien-être et du développement social du mineur, de considérations tenant à la sûreté et à la sécurité et de l'avis du mineur en fonction de son âge et de sa maturité »[137].

D'une façon générale, le considérant 48 de l'AI Act souligne « le fait que les enfants bénéficient de droits spécifiques consacrés à l'article 24 de la Charte et dans la convention des Nations unies relative aux droits de l'enfant (et précisés dans l'observation générale nº 25 de la CNUDE en ce qui concerne l'environnement numérique), et que ces deux textes considèrent la prise en compte des vulnérabilités des enfants et la fourniture d'une protection et de soins appropriés comme nécessaires au bien-être de l'enfant ».

ii. Les risques d'atteinte par les SIA

79. Premier facteur de risque : la vulnérabilité des enfants. Les enfants étant particulièrement vulnérables, une attention particulière doit être portée sur le fonctionnement du SIA dès lors qu'il est susceptible d'interagir avec des *enfants*. Ainsi que l'indique l'AI Act, des SIA peuvent exploiter les vulnérabilités d'une personne ou d'un groupe particulier de personnes en raison de leur âge et risquent de leur causer un préjudice (AI Act, cons. 29 ; v. égal. art. 5, §1, b).

L'article 9, §9 de l'AI Act préconise de prendre « en considération la probabilité que, compte tenu de sa destination, le système d'IA à haut risque puisse avoir une incidence négative sur des personnes âgées de moins de 18 ans » lors de la mise en œuvre du système de gestion des risques. En effet, les enfants peuvent ne pas avoir les capacités leur permettant de comprendre le fonctionnement d'un SIA et les dommages matériels, moraux ou corporels que l'utilisation du SIA peut provoquer.

80. Deuxième facteur de risque : les données à caractère personnel concernant des enfants. Les *données à caractère personnel* concernant des enfants bénéficient d'une protection particulière en droit de l'Union. Tout d'abord, le règlement 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (ci-après, RGPD)[138] encadre strictement les traitements de données

concernant des enfants fondés sur les intérêts légitimes du responsable du traitement ou de tiers[139] et les conditions dans lesquelles un enfant peut consentir au traitement des données à caractère personnel le concernant[140]. Il prévoit ensuite un régime spécial pour le droit à l'effacement des données collectées sur le fondement du consentement de l'enfant[141]. Ainsi, un SIA traitant des données concernant des enfants doit respecter des dispositions particulières pour garantir leur droit à la protection des données.

c. Le droit d'intégration des personnes handicapées (art. 26 de la Charte)

> *CHARTE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE*
> *ARTICLE 26 - INTEGRATION DES PERSONNES HANDICAPEES*
> *L'UNION RECONNAIT ET RESPECTE LE DROIT DES PERSONNES HANDICAPEES A BENEFICIER DE MESURES VISANT A ASSURER LEUR AUTONOMIE, LEUR INTEGRATION SOCIALE ET PROFESSIONNELLE ET LEUR PARTICIPATION A LA VIE DE LA COMMUNAUTE.*

i. Le cadre juridique

81. Une portée limitée. L'article 26 de la Charte semble davantage consister en l'énoncé d'un principe qu'en la consécration d'un droit subjectif pour les personnes handicapées[142]. Cette interprétation a été confirmée par la CJUE dans l'arrêt *Glatzel* du 22 mai 2014, indiquant que le principe d'intégration des personnes handicapées « n'implique pas […] que le législateur de l'Union soit tenu d'adopter telle ou telle mesure particulière » et qu' « afin que cet article produise pleinement ses effets, il doit être concrétisé par des dispositions du droit de l'Union ou du droit national. Par conséquent, ledit article ne saurait, en lui-même, conférer aux particuliers un droit subjectif invocable en tant que tel »[143].

Toutefois, cet article n'est pas privé de toute efficacité. En effet, la CJUE a affirmé que l'obligation pour les employeurs de prévoir des aménagements raisonnables pour les personnes handicapées « doit être lue à la lumière de l'article 26 de la Charte qui énonce le principe d'intégration des personnes handicapées afin qu'elles bénéficient de mesures visant à assurer leur autonomie, leur intégration sociale et professionnelle et leur participation à la vie de la communauté »[144]. Ainsi, l'article 26 de la Charte pourrait être utilisé dans le cadre de la mise en œuvre des dispositions de l'AI Act relatives aux personnes handicapées.

ii. Les risques d'atteinte par les SIA

82. Facteur de risque : l'accessibilité. Les *personnes handicapées* sont confrontées à la problématique spécifique de l'accessibilité.

L'accessibilité est définie par l'article 9 de la Convention des Nations Unies relative aux droits des personnes handicapées comme la capacité pour les « personnes handicapées de vivre de façon indépendante et de participer pleinement à tous les aspects de la vie » en leur garantissant « l'accès à l'environnement physique, aux transports, à l'information et à la communication, y compris aux systèmes et technologies de l'information et de la communication, et aux autres équipements et services ouverts ou fournis au public, tant dans les zones urbaines que rurales »[145]. En droit de l'Union, les obligations en termes d'accessibilité

sont prévues par les directives 2016/2102 du 26 octobre 2016 relative à l'accessibilité des sites internet et des applications mobiles des organismes du secteur public[146] et 2019/882 du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services[147].

L'AI Act souligne l'importance de l'accessibilité des SIA pour les personnes handicapées. L'accessibilité des SIA dépend fortement de la qualité, de la forme et du contenu des informations communiquées aux personnes handicapées (AI Act, cons. 142 et 165)[148].

Ainsi, dès lors qu'un SIA est susceptible d'interagir avec des *personnes handicapées*, il convient de veiller à ce que le SIA soit accessible, notamment lorsque le SIA est utilisé dans des domaines cruciaux pour les personnes comme l'*accès aux services publics* ou à l'*éducation et à la formation*.

---

[88] MOLINIER Joël (dir.), *Les principes fondateurs de l'Union européenne*, Paris : Puf, coll. Droit et justice, 2005, p. 233

[89] Dir. 2000/43 du 29 juin 2000 relative à la mise en œuvre du principe de l'égalité de traitement entre les personnes sans distinction de race ou d'origine ethnique, *JOCE*, L 180, 19 juill. 2000, p. 22-26

[90] MOLINIER Joël (dir.), *Les principes fondateurs de l'Union européenne*, Paris : Puf, coll. Droit et justice, 2005, p. 233

[91] CJUE, 1er mars 2011, *Test-Achats* et al., aff. C-236/09

[92] CJUE, 1er mars 2011, Test-Achats *et al*., aff. C-236/09

[93] TINIERE Romain et VIAL Claire, *Droit de l'Union européenne des droits fondamentaux*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 2023, p. 471

[94] CJUE, 16 déc. 2008, Arcelor Atlantique et Lorraine *et al*., C-127/07

[95] BRIBOSIA Emmanuelle, RORIVE Isabelle et HISLAIRE Julien, « Article 21 Non-discrimination », *In* PICOD Fabrice et RIZCALLAH Cecilia et VAN DROOGHENBROECK Sébastien (dir.), *Charte des droits fondamentaux de l'Union européenne : Commentaire article par article*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 3ème éd., 2023, p. 619

[96] V. CJUE, 14 janv.2021, Staatssecretaris van Justitie en Veiligheid, aff. C-441/19 : Dans cette affaire, le juge européen a choisi de viser l'article 24 de la Charte pour préciser les conditions de retour d'un mineur non accompagné alors que la question préjudicielle se fondait sur l'article 21 de la Charte.

[97] V. CJUE, 21 oct. 2021, Komisia zashtita ot diskriminatsia, aff. C-824/19 : La Cour a inclus d'office « une référence aux articles 21 et 26 de la Charte dans une question préjudicielle qui se fondait sur la directive 2000/78 et la Convention des Nations unies relative aux droits des personnes handicapées et l'interprétation de l'obligation d'aménagement raison- nable à la lumière de l'article 26 de la Charte qui énonce le principe d'intégration des personnes handicapées » (BRIBOSIA Emmanuelle, RORIVE Isabelle et HISLAIRE Julien, « Article 21 Non-discrimination », *In* PICOD Fabrice et RIZCALLAH Cecilia et VAN DROOGHENBROECK Sébastien (dir.), *Charte des droits fondamentaux de l'Union européenne : Commentaire article par article*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 3ème éd., 2023, p. 621).

[98] BRIBOSIA Emmanuelle, RORIVE Isabelle et HISLAIRE Julien, « Article 21 Non-discrimination », *In* PICOD Fabrice et RIZCALLAH Cecilia et VAN DROOGHENBROECK Sébastien (dir.), *Charte des droits fondamentaux de l'Union européenne : Commentaire article par article*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 3ème éd., 2023, p. 623-624

[99] A l'inverse de la liste de l'article 19 du TFUE énonçant que « sans préjudice des autres dispositions des traités et dans les limites des compétences que ceux-ci confèrent à l'Union, le Conseil, statuant à l'unanimité conformément à une procédure législative spéciale, et après approbation du Parlement européen, peut prendre les mesures nécessaires en vue de combattre toute discrimination fondée sur le sexe, la race ou l'origine ethnique, la religion ou les convictions, un handicap, l'âge ou l'orientation sexuelle ». V. MARTIN Denis, « Fasc. 602 : Article 19 TFUE, articles 20 et 21 de la Charte des droits fondamentaux et lutte contre les discriminations », *J.-Cl. Europe Traité*, 2021, n° 20 et s.

[100] V. dir. 2023/970 du 10 mai 2023 visant à renforcer l'application du principe de l'égalité des rémunérations entre les femmes et les hommes pour un même travail ou un travail de même valeur par la transparence des rémunérations et les mécanismes d'application du droit, *JOUE,* L 132, 17 mai 2023, p. 21-44

[101] V. dir. 2010/41 du 7 juillet 2010 ; dir. 2004/113/CE du 13 déc. 2004 mettant en œuvre le principe de l'égalité de traitement entre les femmes et les hommes dans l'accès à des biens et services et la fourniture de biens et services, *JOUE,* L 373, 21 déc. 2004, p. 37-43

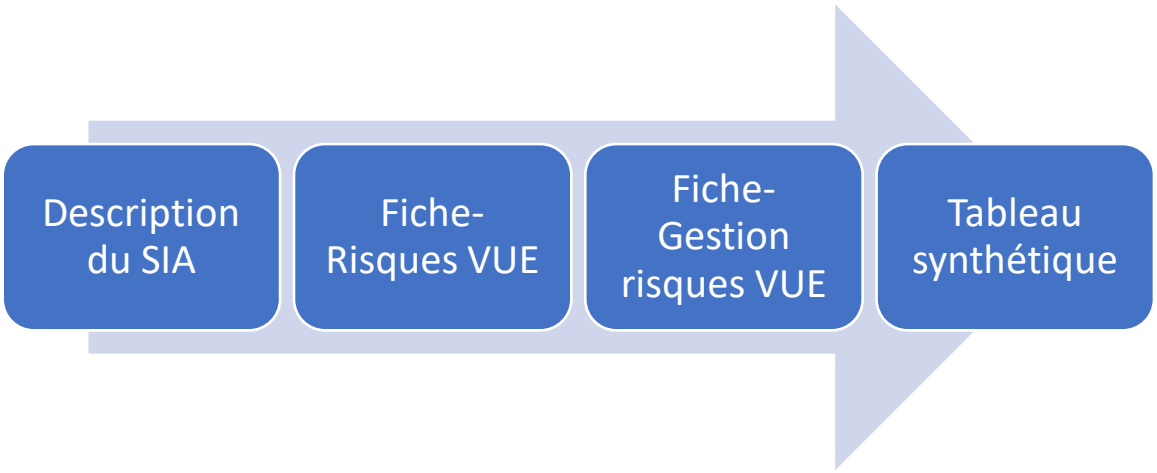
[102] V. dir. 2022/2381 du 23 nov. 2022 relative à un meilleur équilibre entre les femmes et les hommes parmi les administrateurs des sociétés cotées et à des mesures connexes, *JOUE,* L 315, 7 déc. 2022, p. 44-59
[103] CJUE, 1er mars 2011, Test-Achats *et al*., aff. C-236/09
[104] Dir. 2023/970 du 10 mai 2023, art. 1
[105] Dir. 2004/113/CE du 13 déc. 2004, art. 4
[106] Dir. 2004/113/CE du 13 déc. 2004, art. 2
[107] GARRONE Pierre, « La discrimination indirecte en droit communautaire : vers une théorie générale », *RTD eur*, 1994, n°3, p. 425
[108] Dir. 2004/113/CE du 13 déc. 2004, art. 6
[109] Selon la CJUE, le droit de l'Union ne s'oppose « pas à une règle nationale qui oblige, à qualifications égales des candidats de sexe différent quant à leur aptitude, à leur compétence et à leurs prestations professionnelles, à promouvoir prioritairement les candidats féminins dans les secteurs d'activité du service public où les femmes sont moins nombreuses que les hommes au niveau de poste considéré, à moins que des motifs tenant à la personne d'un candidat masculin ne fassent pencher la balance en sa faveur, à condition que : - elle garantisse, dans chaque cas individuel, aux candidats masculins ayant une qualification égale à celle des candidats féminins que les candidatures font l'objet d'une appréciation objective qui tient compte de tous les critères relatifs à la personne des candidats et écarte la priorité accordée aux candidats féminins, lorsqu'un ou plusieurs de ces critères font pencher la balance en faveur du candidat masculin, et - de tels critères ne soient pas discriminatoires envers les candidats féminins » (CJUE, 11 nov. 1997, Marschall, aff. C-409/95).
[110] CJCE, 30 avril 1996, P. c/ S. et Cornwall City Council, C-13/94
[111] Dir. 2000/43 du 29 juin 2000, art. 2, 2
[112] Dir. 2000/43 du 29 juin 2000, art. 3, 1
[113] Dir. 2000/43 du 29 juin 2000, art. 5
[114] CJUE, 13 oct. 2022, S.C.R.L. (Vêtement à connotation religieuse), aff. C-344/20 ; CJUE, 15 juill. 2021, Wabe, aff. C-804/18 et C-341/19
[115] Dir. 2000/78/CE du 27 novembre 2000 portant création d'un cadre général en faveur de l'égalité de traitement en matière d'emploi et de travail, *JOCE L* 303, 2 déc. 2000, p. 16-22
[116] CJUE, 14 mars 2017, G4S Secure Solutions NV, aff. C-157/15
[117] CJUE, 13 oct. 2022, S.C.R.L. (Vêtement à connotation religieuse), aff. C-344/20
[118] CJCE, 11 juill. 2006, Chacón Navas, aff. C-13/05, pt. 44
[119] CJCE, 11 juill. 2006, Chacón Navas, aff. C-13/05, pt. 43
[120] CJCE, 11 juill. 2006, Chacón Navas, aff. C-13/05, pt. 45
[121] CJUE, 18 déc. 2014, FOA, aff. C-354/13
[122] CJCE, 17 juill. 2008, Coleman, aff. C-303/06
[123] CJUE, 22 mai 2014, Glatzel, aff. C-356/12
[124] Le partenariat de vie a été créé en Allemagne en 2001. Il est comparable au Pacs français. V. Sénat, *Les documents de travail du Sénat, série législation comparée – Le mariage homosexuel*, 2004, n° LC 134, p. 9
[125] CJUE, 1er avr. 2008, Maruko, aff. C-267/06 ; dans le même sens, CJUE, 12 déc. 20013, Hay, aff. C-267/12
[126] CJUE, 29 avr. 2015, Léger, aff. C-528/13
[127] Dir. 2000/43/CE du 29 juin 2000, art. 3, 2
[128] Explications relatives à la Charte des droits fondamentaux, *JOUE,* C 303, 14 déc. 2007, p. 17
[129] BRIBOSIA Emmanuelle, RORIVE Isabelle et HISLAIRE Julien, « Article 21 Non-discrimination », *In* PICOD Fabrice et RIZCALLAH Cecilia et VAN DROOGHENBROECK Sébastien (dir.), *Charte des droits fondamentaux de l'Union européenne : Commentaire article par article*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 3ème éd., 2023, p. 632
[130] CJCE, 30 mai 1989, Commission c/ Grèce, aff. 305/87
[131] V. art. 2, §34 sur la notion de données biométriques et 40 relatif au système d'IA de catégorisation biométrique.
[132] Dir. 2011/93 du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil, *JOUE*, L 335, 17 déc. 2011, p. 1-14
[133] Unicef, « La Convention Internationale des Droits de l'Enfant (CIDE) ». Disponible sur : https://www.unicef.fr/convention-droits-enfants/
[134] Règl. 2019/1111 du 25 juin 2019 relatif à la compétence, la reconnaissance et l'exécution des décisions en matière matrimoniale et en matière de responsabilité parentale, ainsi qu'à l'enlèvement international d'enfants, *JOUE*, L 178, 2 juin 2019, p. 1-115, dit Bruxelles II ter ; Dir. 2011/95 du 13 déc. 2011 concernant les normes relatives aux conditions que doivent remplir les ressortissants des pays tiers ou les apatrides pour pouvoir bénéficier d'une protection internationale, à un statut uniforme pour les réfugiés ou les personnes pouvant bénéficier de la protection subsidiaire, et au contenu de cette protection, *JOUE*, L 337, 20 déc. 2011, p. 9-26 ; Dir. 2008/115/CE du 16 déc. 2008 relative aux normes et procédures communes applicables dans les États membres au retour des ressortissants de pays tiers en séjour irrégulier, *JOUE*, L 348, 24 déc. 2008, p. 98-107

[135] CJUE, 11 mars 2021, Etat belge (Retour du parent d'un mineur), aff. C-112/20 ; CJUE, 23 décembre 2009, Deticek c. Sgueglia, aff. C-403/09 ; CJCE, 27 juin 2006, Parlement c. Conseil, aff. C-540/03
[136] V. par ex. dir. 2012/29 du 25 oct. 2012 établissant des normes minimales concernant les droits, le soutien et la protection des victimes de la criminalité et remplaçant la décision-cadre 2001/220/JAI du Conseil, *JOUE*, L 315, 14 nov. 2012, p. 57-73, art. 1er, 2 : « Les Etats membres veillent à ce que, lorsqu'il s'agit d'appliquer la présente directive et que la victime est un enfant, l'intérêt supérieur de l'enfant soit une considération primordiale, évaluée au cas par cas. Une approche axée spécifiquement sur l'enfant, tenant dûment compte de son âge, de sa maturité, de son opinion, de ses besoins et de ses préoccupations, est privilégiée ».
[137] Dir. 2011/93 du 13 déc. 2011, cons. 18
[138] Règl. 2016/679 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, et abrogeant la directive 95/46/CE, *JOUE*, L 119, 4 mai 2016, p. 1-88
[139] RGPD, art. 6, 1, f) et cons. 38
[140] RGPD, art. 8
[141] RGPD, art. 17, 1, f) et cons. 65
[142] V. ANDREEA MACOVEI Oana, « L'intégration des personnes handicapées dans l'Union européenne – Quel bilan ? », *Rev. UE*, 2016, p. 37 ; TINIERE Romain et VIAL Claire, Droit de l'Union européenne des droits fondamentaux, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 2023, p. 535 et s.
[143] CJUE, 22 mai 2014, Glatzel, aff. C-356/12, pt. 78
[144] CJUE, 21 oct. 2021, Komisia zashtita ot diskriminatsia, aff. C-824/19 ; v. égal. CJUE, 10 févr. 2022, aff. C-485/20
[145] Conseil de l'Europe, *Stratégie du Conseil de l'Europe sur le handicap 2017-2023*, 2016, p. 23
[146] Dir. 2016/2102 du 26 octobre 2016 relative à l'accessibilité des sites internet et des applications mobiles des organismes du secteur public, *JOUE*, L 327, 2 déc. 2016, p. 1–15.
[147] Dir. 2019/882 du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services, *JOUE*, L 151, 7 juin 2019, p. 70–115.
[148] V. égal. Unesco, Recommandation sur l'éthique de l'intelligence artificielle, 2021, pt. 106

B. L'étude d'impact

83. Présentation. L'étude d'impact se déroule en trois étapes :

- la première étape consiste à *décrire le SIA* ;
- la deuxième étape vise à réaliser une *Fiche-Risques VUE* (annexe 5) qui rend compte de l'analyse des risques qu'un SIA donné pourrait engendrer pour les VUE ;
- la troisième étape conduit à déterminer des *mesures de gestion des risques* et une *Fiche-Gestion risques VUE* (annexe 6) permettant de réduire le niveau des risques à un degré acceptable ;
- l'ensemble des résultats de ce processus doit être consigné dans un *Tableau synthétique de l'étude d'impact* (annexe 7), à titre d'information des déployeurs.



1. Étape 1 : La description du SIA : Tableau descriptif du SIA (annexe 4)

84. La première phase de l'étude d'impact : une description du SIA. La description du SIA constitue la première phase de l'étude d'impact sur les VUE. Elle vise à décrire le projet dans une double dimension[149] :

- une description des tâches et des responsabilités des personnes impliquées dans chacune des étapes du projet ;
- une description du SIA lui-même, y compris dans son contexte potentiel de déploiement.

85. Une étape nécessaire pour l'identification des VUE potentiellement affectées. La description du SIA consiste à expliquer précisément la destination et/ou les finalités, les fonctions et les modalités spécifiques de fonctionnement et d'utilisation du SIA[150]. Il s'agit d'une « fiche d'identité » du SIA. Elle permet de répartir clairement les tâches et les responsabilités des personnes impliquées dans la conception, la validation et la vérification, le déploiement et l'exploitation et le suivi du SIA. Elle doit servir de base d'informations pour la réalisation de la *Fiche-Risques VUE* (étape 2 de l'étude d'impact). En particulier, les réponses aux questions posées pour réaliser la description peuvent permettre de repérer les VUE

potentiellement affectées par le SIA (dans son fonctionnement et/ou dans son déploiement/utilisation).

Objectifs de la description du SIA	Une description détaillée des :
• Présenter formellement les caractéristiques du SIA • Répartir les tâches et les responsabilités des acteurs • Identifier les VUE potentiellement affectées par le SIA	• Destination et finalités : les causes pour lesquelles le SIA est développé, les besoins qu'il cherche à satisfaire ; • Fonctions : tâches que le SIA effectue ; • Modalités de fonctionnement ou d'utilisation : objets ou personnes concernées par le SIA, contexte de déploiement du SIA, technologies utilisées et étendue de l'utilisation (en termes d'objet, temporel et géographique)

86. Une liste de questions au sein d'un tableau descriptif. La description du SIA consiste à donner des informations le concernant, sur la base d'une série de questions regroupées dans un *Tableau descriptif du SIA* (Annexe 4). Les réponses à ces questions doivent être courtes et précises et doivent idéalement comporter quelques mots-clefs, qui permettront de se reporter facilement à la cartographie des VUE.

87. Les objets des questions. Les questions ont trois cibles prioritaires, issues de la lecture de l'AI Act. Il s'agit principalement de décrire les fonctions, les finalités et les modalités de fonctionnement et d'utilisation du SIA. Ainsi, il y a trois questions principales (quelles sont les fonctions du SIA, quelles sont ses finalités et quelles sont ses modalités spécifiques ?) se déclinant en une série de questions plus précises dans le cadre de la méthode des 5 W ou QQOQCCP (Qui ? Quoi ? Où ? Quand ? Comment ? Combien ? Pourquoi ?).

Les questions peuvent être regroupés dans les catégories suivantes :

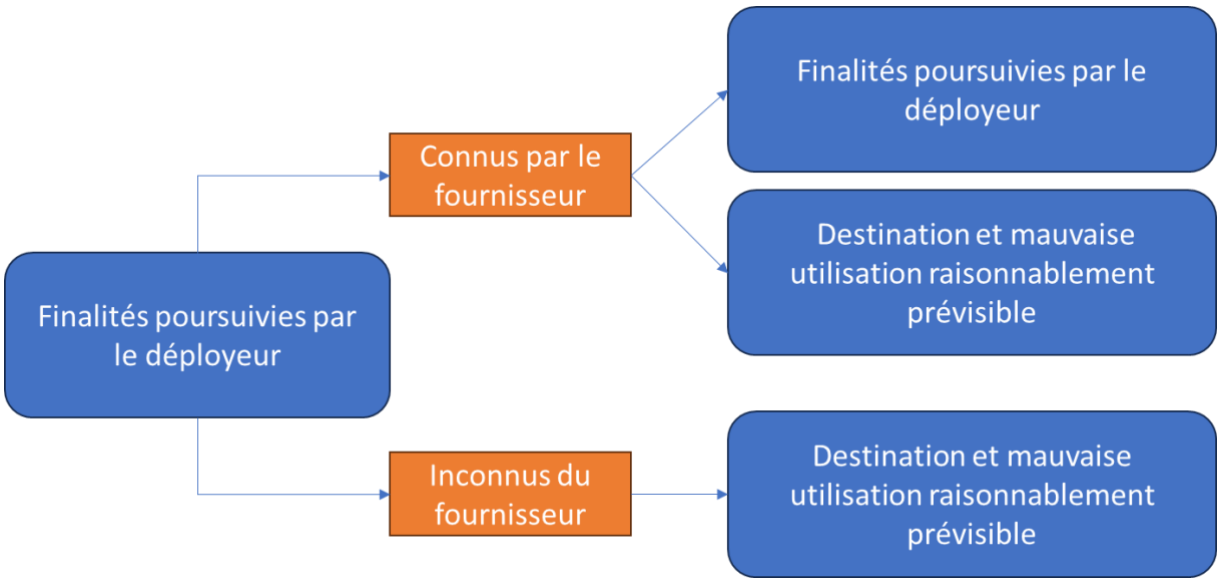
1. Les personnes impliquées dans le cycle de vie du SIA
2. La destination du SIA et les finalités
3. Les fonctions du SIA
4. Les objets traités par le SIA
5. Le contexte dans lequel évolue le SIA (matériel, spatial et temporel)
6. Les technologies utilisées
7. La description scalaire de déploiement du SIA (en termes géographique, temporel et d'objets/de personnes)

88. La distinction entre la destination et les finalités. Il est important de rappeler la différence terminologique entre la destination du SIA et les finalités et ses implications.

La destination est définie par l'AI Act comme « l'utilisation à laquelle un système d'IA est destiné par le fournisseur, y compris le contexte et les conditions spécifiques d'utilisation, tels qu'ils sont précisés dans les informations communiquées par le fournisseur dans la notice d'utilisation, les indications publicitaires ou de vente et les déclarations, ainsi que dans la documentation technique » (AI Act, art. 3, §12). La destination est donc définie par le fournisseur. La finalité, quant à elle, correspond aux besoins du déployeur, les raisons pour lesquelles il souhaite avoir recours à ce SIA spécifique. Idéalement, il convient de prendre en compte la finalité car elle assure une prise en compte « en contexte » de l'usage concret du SIA. Néanmoins, le fournisseur peut développer un SIA sans avoir de connaissance précise des finalités motivant le déployeur. Le SIA peut ainsi être développé pour réaliser certaines tâches ou actions mais sans connaître les usages spécifiques futurs du SIA, propres aux besoins du déployeur. Dans ce cas, il est fait référence à la destination. Il convient de préciser l'ensemble des destinations s'il y en a plusieurs.

En outre, l'AI Act impose aux fournisseurs de prendre en compte la « mauvaise utilisation raisonnablement prévisible » du SIA. Cette notion est définie par l'article 3, §13 de l'AI Act comme « l'utilisation d'un système d'IA d'une manière qui n'est pas conforme à sa destination, mais qui peut résulter d'un comportement humain raisonnablement prévisible ou d'une interaction raisonnablement prévisible avec d'autres systèmes, y compris d'autres systèmes d'IA ». Il faut alors non seulement prendre en compte les usages conformes à la destination du SIA mais aussi les autres usages pouvant découler des fonctions du SIA. Partant, il est nécessaire de décrire le SIA au regard de sa destination mais également des mauvaises utilisations raisonnablement prévisibles.

La destination et les mauvaises utilisations raisonnablement prévisibles doivent, en outre, être pris en compte dans l'hypothèse où les finalités poursuivies par le déployeur ne sont pas connues. En effet, même dans cette hypothèse, le fournisseur doit définir la destination du SIA (même s'il n'a pas connaissance des finalités) et prévoir les cas de mauvaises utilisations dans le cadre de la gestion des risques.



2. Étape 2 : L'analyse des risques : Fiche-risques VUE (annexe 5)

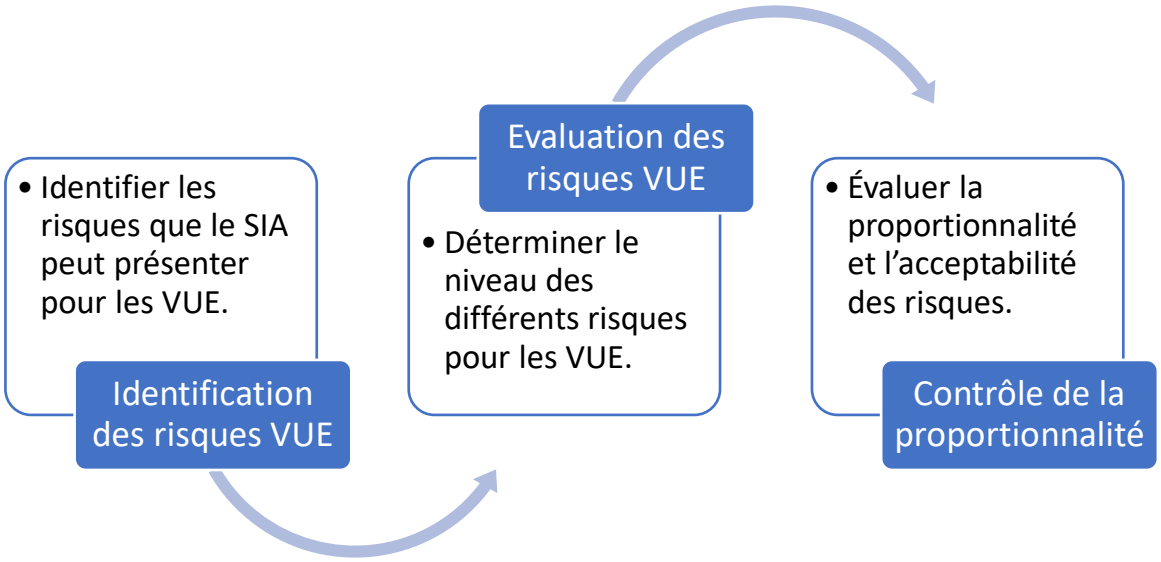
89. La deuxième phase de l'étude d'impact : l'analyse des risques. Cette étape consiste à identifier les risques pour les VUE que présente le SIA dans la perspective de les réduire, voire de les éliminer, en particulier si cela s'avère nécessaire du fait de leur nature disproportionnée. A cette fin, il s'agit de déterminer si les risques sont acceptables. En effet, l'AI Act n'impose pas que les SIA ne présentent aucun risque mais que ceux-ci, s'il y en a, soient acceptables[151]. L'acceptabilité du risque découle de sa proportionnalité aux autres intérêts que le SIA met en œuvre. En cas de disproportion entre le risque d'atteinte aux VUE et les intérêts mis en œuvre par le SIA, le risque doit être considéré comme étant inacceptable. Si un risque s'avère en première analyse inacceptable, il est alors nécessaire de mettre en place des mesures de gestion des risques destinées à rendre ce risque acceptable. Pour établir que le risque est acceptable, c'est-à-dire proportionné, il faut réaliser un contrôle de proportionnalité.

Partant, cette phase d'analyse des risques comporte trois volets :

- identifier formellement les risques pour les VUE ;
- évaluer les niveaux des risques ;
- réaliser un contrôle de la proportionnalité entre le risque et les intérêts poursuivis par le SIA.

Elle prend appui sur la *Fiche-Risques VUE* dont la mise en pratique nécessite d'utiliser la description du SIA (*Tableau descriptif du SIA*), effectuée à l'étape 1, et sur la cartographie des VUE (v. *supra*, II, A) et l'*Index des risques*.

A l'issue de l'étape 2, un score de risque est déterminé pour le SIA permettant de s'orienter vers la gestion des risques (étape 3).

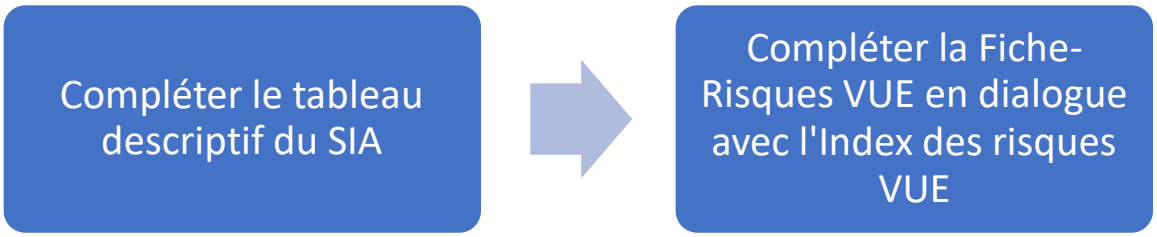


90. La description et l'utilisation de la Fiche-Risques VUE. Le plan de la *Fiche-Risques VUE* suit les étapes de l'analyse des risques. Ainsi, en premier lieu, il s'agit de décrire le risque puis, en second lieu, d'effectuer le contrôle de proportionnalité.

Des questions, en lien avec la présente méthodologie, permettent de guider ce travail d'analyse.

Par exemple :

Si à une question du tableau descriptif la réponse est « *vie privée* », il faut rechercher dans la cartographie des VUE, et plus précisément dans l'*Index des risques VUE*, les éléments « *vie privée* ».



91. Une analyse individuelle pour chaque risque identifié. Chaque risque VUE doit faire l'objet d'une analyse distincte. Il convient ainsi de faire une Fiche différente pour chacun des risques identifiés. Il est possible d'analyser ensemble plusieurs risques s'ils sont relatifs au même droit ou principe fondamental de concrétisation (s'ils se trouvent dans la même case de l'*Index des risques*).

a. L'identification des risques VUE

92. L'articulation entre le tableau descriptif, l'Index des risques VUE et la Fiche-Risques VUE. L'identification des risques VUE du SIA nécessite de suivre la démarche suivante :

- Comparer les réponses du *Tableau descriptif du SIA* avec l'*Index des risques VUE* ;
- Puis reporter les correspondances entre le *Tableau descriptif du SIA* et l'*Index des risques* dans la *Fiche-Risques VUE*.

Référence Fiche-Risques VUE :

1) Quel est le facteur de risque que présente le SIA ?

Il s'agit de reporter les mots-clefs de l'Index des risques correspondants à des éléments figurant dans le Tableau descriptif.

2) Quelles sont les valeurs de l'Union européenne potentiellement menacées ?

Il s'agit de la VUE se trouvant sur la même ligne que le mot-clef de l'Index des risques.

93. En cas d'impossibilité d'identifier les risques. Les réponses aux questions peuvent ne pas permettre d'identifier un risque dans deux situations :

- Soit la réponse semble constituer un facteur de risque mais il n'y a pas de correspondance immédiate entre la réponse et les risques répertoriés dans l'*Index* :

- Il est possible de retenir un risque similaire par analogie et dans cette hypothèse, ce risque pourra être retenu ;
- A défaut d'analogie possible, il convient de se reporter à l'article 2 du TUE afin d'identifier les valeurs pouvant être mises en jeu et, à l'aune de la Charte des droits fondamentaux de l'UE (et de la jurisprudence y afférente), le ou les droits et principes fondamentaux de concrétisation.

Article 2 du TUE :	Charte des droits fondamentaux de l'Union européenne :
L'Union est fondée sur les valeurs de respect de la dignité humaine, de liberté, de démocratie, d'égalité, de l'État de droit, ainsi que de respect des droits de l'homme, y compris des droits des personnes appartenant à des minorités. Ces valeurs sont communes aux États membres dans une société caractérisée par le pluralisme, la non-discrimination, la tolérance, la justice, la solidarité et l'égalité entre les femmes et les hommes.	Le site de l'Agence des droits fondamentaux de l'Union européenne présente la Charte article par article ainsi que la jurisprudence (https://fra.europa.eu/fr/eu-charter). La Charte est reproduite en annexe (annexe 2).

- Soit la réponse ne semble pas constituer un facteur de risque : dans ce cas, il convient de continuer l'étude d'impact sans tenir compte de cette réponse.

94. La réalisation de tests à l'appui de l'identification des risques VUE. L'identification des risques VUE peut être améliorée grâce à la réalisation de test du SIA. Les tests peuvent permettre d'identifier précisément la nature et l'importance des risques VUE. Par exemple, les tests peuvent révéler un taux élevé de faux positifs qui, dans certaines circonstances, peut constituer un risque VUE.

La réalisation de tests est par ailleurs préconisée par l'article 9, §8 de l'AI Act (dans le contexte de l'élaboration d'un système de gestion des risques par le fournisseur d'un SIA à haut risque). Des tests peuvent donc être utilement effectués à la fois aux fins de conformité à l'AI Act et aux VUE.

b. L'évaluation des risques VUE

95. L'évaluation des risques se décompose en deux étapes. En premier lieu, il faut estimer le niveau de risque (i) et, en second lieu, il faut établir la proportionnalité du risque (ii).

i. Evaluer le niveau de risque VUE

96. Le niveau de risque dépend de la sévérité et de la probabilité du préjudice. La gravité du préjudice est appréciée au regard des critères des conséquences et de l'ampleur du préjudice. Quant à la probabilité du préjudice, elle dépend principalement des caractéristiques techniques du SIA mais il faut aussi prendre en compte l'effet de certaines exigences

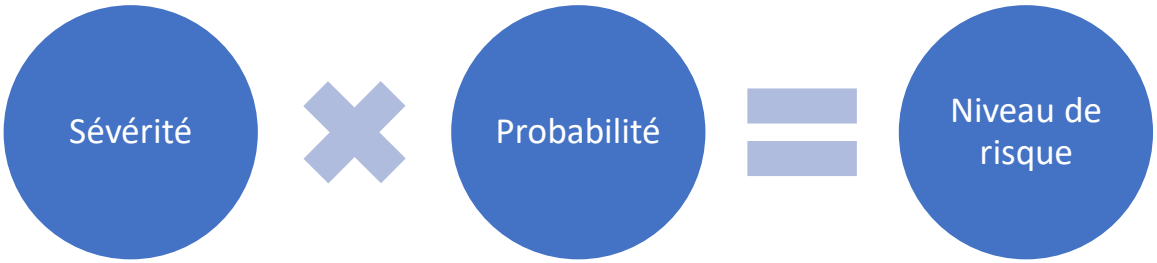
essentielles de l'AI Act (exigences imposées aux SIA à haut risque par les articles 10 à 15 de l'AI Act). La combinaison de l'ensemble de ces facteurs permet d'obtenir le niveau de chaque risque VUE appliqué au SIA.

Une analyse du niveau de risque doit être effectuée pour chacun des risques identifiés au préalable.

- La combinaison des critères de la sévérité et de la probabilité du préjudice :

97. Les critères d'évaluation du niveau de risque : la sévérité et la probabilité du préjudice. L'AI Act définit le risque comme « la combinaison de la probabilité d'un préjudice et de la sévérité de celui-ci ». L'évaluation du niveau de risque consiste donc à combiner ces deux facteurs, combinaison qui pourrait être retranscrite ainsi : sévérité du préjudice*probabilité du préjudice = niveau de risque[152].

Cette méthode de détermination du niveau de risque peut être rapprochée de celle utilisée dans le cadre d'une analyse d'impact relative à la protection des données. Le niveau de risque y est apprécié par rapport à la gravité et à la vraisemblance d'un risque[153].



98. Le préjudice. D'une façon générale, en droit, le préjudice est une atteinte portée à la personne elle-même – le préjudice dans ce cas peut être corporel ou moral – ou aux biens de la personne – il s'agit du préjudice matériel. Il faut ajouter une autre hypothèse de préjudice, qui n'affecte pas une personne déterminée mais la collectivité, qui est le préjudice écologique, notamment introduit dans le Code civil français en 2016[154].

A l'aune de ce contexte générique, il convient de préciser la notion de préjudice, ou de dommage[155], au sens de l'AI Act. Le considérant 5 de l'AI Act indique que « l'IA peut générer des risques et porter atteinte aux intérêts publics et aux droits fondamentaux protégés par le droit de l'Union. Le préjudice causé peut être matériel ou immatériel, y compris physique, psychologique, sociétal ou économique ». Ce considérant vise donc tous les types de préjudice, à savoir matériel (préjudice économique), moral (préjudice psychologique) et corporel (préjudice physique). Il faut souligner la mention d'un préjudice « sociétal » qui ne renvoie pas à un préjudice individuel mais un préjudice affectant la collectivité. Il pourrait s'agir d'atteintes affectant le fonctionnement de la société, et notamment son fonctionnement démocratique (AI Act, cons. 27). En ce sens, le dommage sociétal peut être considéré comme une atteinte directe aux VUE, au-delà de la violation d'un droit fondamental dans un cas individuel. Enfin, l'article 2, §49 de l'AI Act évoque les dommages à l'environnement, impliquant la prise en compte du préjudice environnemental par ce texte.

Enfin, il faut préciser la notion de « préjudice éventuel » évoqué par le considérant 52. Le préjudice éventuel est un préjudice hypothétique, qui n'est pas certain. En l'occurrence, la référence au préjudice éventuel est nécessaire en ce qu'il s'agit de prévenir un préjudice qui pourrait être causé aux utilisateurs finaux. Aussi, la prise en compte du préjudice éventuel est nécessaire pour déterminer le niveau de risque.

Préjudice	Matériel Atteinte causé aux biens, préjudice économique
	Immatériel Atteinte psychologique
	Corporel Atteinte physique, à la santé et à la sécurité
	Environnemental Atteinte causé à l'environnement
	Sociétal Atteinte causé au fonctionnement de la société

Référence Fiche-Risques VUE :
3) Quels sont le ou les préjudices potentiels ?
Il faut indiquer le type de préjudice que risque de provoquer le SIA au regard du tableau présenté ci-dessus.

- La sévérité du préjudice :

99. Le facteur de la sévérité du préjudice. L'AI Act ne donne pas de définition de la sévérité du préjudice. Pour définir la sévérité, il est possible de se référer aux travaux et à la jurisprudence des autorités de contrôle compétentes en matière de traitement de données à caractère personnel concernant l'analyse d'impact relative à la protection des données (AIPD ou *privacy impact assessment* ou PIA) prévue par le RGPD. Selon la Commission nationale de l'informatique et des libertés (ci-après Cnil), autorité de contrôle de la protection des données française, « la gravité représente l'ampleur d'un risque. Elle est essentiellement estimée au regard de la hauteur des impacts potentiels sur les personnes concernées »[156].

La définition de la Cnil donne des indications utiles qui doivent toutefois être adaptées au contexte des risques pour les VUE.

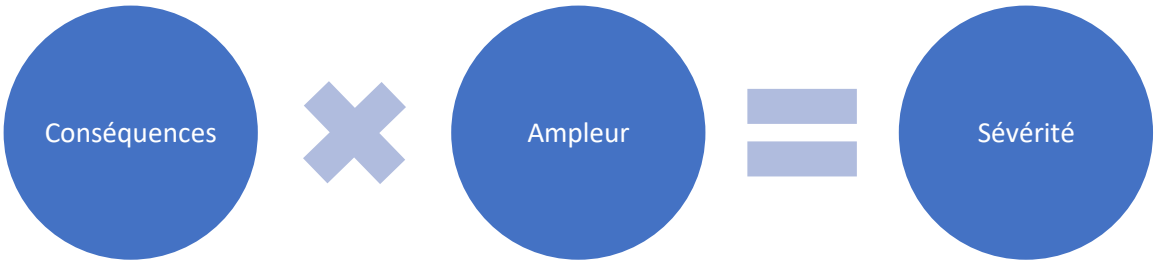
En premier lieu, en ce qui concerne les risques pour les VUE, les conséquences ne sauraient être appréciées uniquement à l'aune des conséquences pour les personnes physiques. Il faut également y inclure les conséquences pour les personnes morales, comme les entreprises,

ou l'État et l'administration mais aussi pour l'environnement. En ce sens, d'abord, les VUE et les droits et principes fondamentaux visent non seulement à protéger les personnes physiques mais aussi les personnes morales. En outre, une atteinte causée aux services de l'État et à l'administration peut avoir des répercussions pour l'ensemble de la société et pourrait donc être considéré comme un préjudice sociétal au sens de l'AI Act. Ensuite, dans le cas du préjudice environnemental, les conséquences du dommage peuvent non seulement affecter les personnes physiques mais aussi les personnes morales, comme les entreprises ou les collectivités territoriales, outre les conséquences directes à l'environnement. Enfin, l'annexe XIII de l'AI Act définit l'impact important sur le marché intérieur en raison de la portée d'un modèle d'IA en prenant en considération les utilisateurs professionnels, lesquels peuvent être des personnes physiques ou morales.

En second lieu, la Cnil apprécie la gravité du risque de façon individuelle, directement par rapport aux personnes concernées prises isolément. Dans la mesure où la protection des VUE consiste à protéger la société européenne et son organisation politique contre des atteintes résultant de risques systémiques, il convient de définir la gravité dans ce cadre systémique. En d'autres termes, cela signifie que la gravité doit être appréciée à la fois individuellement (à l'aune des atteintes individuelles à tel ou tel droit fondamental) mais aussi collectivement (à l'aune des atteintes systémiques à tel ou tel droit ou principe fondamental de concrétisation des VUE).

Deux variables doivent donc être prises en compte : les conséquences du risque VUE pour les individus et les personnes morales (« la hauteur des impacts potentiels sur les personnes concernées » en écho à l'expression de la Cnil dans le contexte du RGPD) (1) mais aussi la diffusion du risque dans la société, c'est-à-dire son ampleur (2).

La sévérité pourrait donc être évaluée selon le produit suivant : conséquences du risque*ampleur du risque = sévérité[157].



- Les conséquences du risque VUE

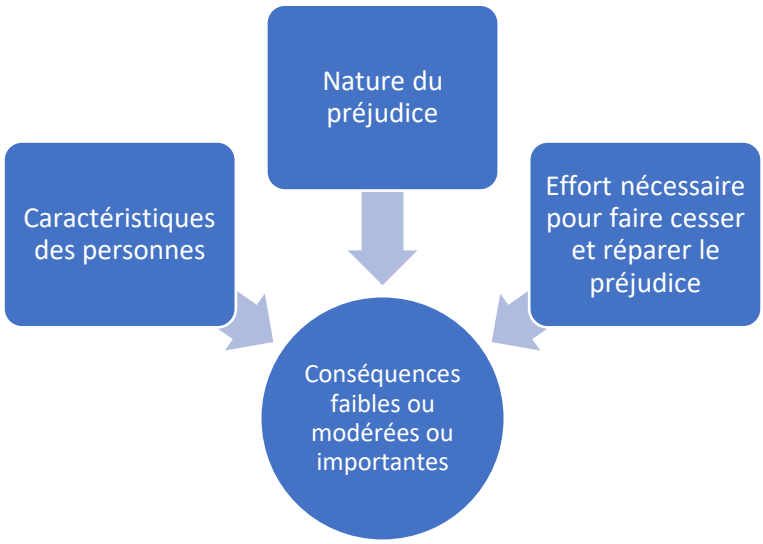
100. Les critères de détermination de l'importance des conséquences. Pour déterminer l'importance des conséquences du risque VUE, plusieurs critères doivent être pris en compte.

Tout d'abord, il convient de déterminer les caractéristiques des personnes concernées et les domaines de leur vie affectés par le SIA. Par exemple, si le risque concerne des activités de consommation de la vie courante, les conséquences seront probablement moins importantes que s'il concerne des personnes malades dans leur accès aux soins ou encore des justiciables.

Ensuite, il faut prendre en compte la nature du préjudice. Le risque de préjudice corporel sera généralement plus grave qu'un risque de préjudice matériel. L'AI Act définit quatre préjudices considérés comme des « incidents graves » (AI Act, art. 2, §49). Il s'agit :

- du décès d'une personne ou d'une atteinte grave à la santé d'une personne ;
- de la perturbation grave et irréversible de la gestion ou du fonctionnement d'infrastructures critiques ;
- de la violation des obligations au titre du droit de l'Union visant à protéger les droits fondamentaux ;
- un dommage grave à des biens ou à l'environnement.

Enfin, il faut tenir compte de l'effort nécessaire pour faire cesser et réparer les conséquences du préjudice[158] : sont-elles facilement ou difficilement surmontables ? Pour cela, il faut notamment prendre en compte les caractéristiques temporelles des conséquences c'est-à-dire la période de temps pendant laquelle les conséquences auront un effet : est-ce un jour, un mois, ou pour une durée indéterminée ? Plus les conséquences négatives durent dans le temps, plus elles doivent être considérées comme étant importantes pour les personnes, la société ou l'environnement. A cet égard, la mise en place de fonctionnalités permettant « l'enregistrement automatique des événements (journaux) tout au long de la durée de vie du système » prévue par l'article 12 de l'AI Act est un élément favorable pour favoriser une réparation rapide du préjudice. En effet, cet enregistrement peut permettre de déceler un fonctionnement anormal du SIA, comme une intrusion dans le système ou un dysfonctionnement ayant causé un préjudice à une personne, et ainsi de corriger le système afin de garantir la protection des VUE en cas d'atteinte.



Référence Fiche-Risques VUE :

4) Quelles sont les victimes potentielles ?

Il faut indiquer les caractéristiques des personnes potentiellement concernées par le préjudice. S'agit-il de personnes physiques ou morales ? De simples consommateurs ? Des patients ou des justiciables ? etc.

5) Quelles sont la nature et l'importance du ou des préjudices ?

Il convient de reprendre la nature du préjudice telle que mentionnée dans la question 3 de la Fiche mais en les décrivant de façon plus précise (types de blessures possibles, biens

matériels susceptibles d'être endommagés, comment la personne peut subir un préjudice moral, etc.)

6) Quel effort est nécessaire pour faire cesser ou réparer le ou les préjudices ?

Il faut indiquer si le préjudice peut facilement être interrompu ou réparé, ou si cela est au contraire difficile. Le décès d'une personne par exemple est un préjudice qui ne peut pas être réparé, il est irréversible.

7) Des dispositifs d'enregistrement conformes à l'article 12 de l'AI Act sont-ils prévus ?

Les dispositifs d'enregistrement peuvent permettre de faciliter la cessation ou la réparation du préjudice. La mise en place d'un préjudice d'enregistrement, outre le fait qu'il s'agisse d'une obligation légale posée par l'article 12 de l'AI Act, est donc un facteur important pour limiter les conséquences du préjudice. Il convient de préciser de quelle façon l'enregistrement peut avoir des effets positifs pour limiter le niveau des conséquences du préjudice.

101. Des conséquences faibles, modérées ou importantes. Sur la base de ces trois éléments, il convient de déterminer si les conséquences du préjudice éventuel sont faibles, modérées ou importantes. Selon les circonstances, les facteurs n'auront pas tous le même poids dans l'appréciation de l'importance des conséquences : ainsi, si le préjudice éventuel implique le décès d'une personne, il faut considérer que les conséquences sont importantes, même si cela concerne des actes de consommation courante (ce qui pourrait être le cas pour des véhicules autonomes), conformément à la définition de l'incident grave donné par l'AI Act. Il s'agit donc d'évaluer précisément, au cas par cas, quelles pourraient être les conséquences et de les mettre en lumière, à l'aune des différents éléments devant être pris en compte.

Le niveau des conséquences doit être chiffré afin de permettre de calculer le score de gravité :

Conséquences	Niveau
Faibles	1
Modérées	2
Importantes	3

- L'ampleur des conséquences des risques VUE

102. Une ampleur individuelle, sectorielle ou systémique. L'ampleur du préjudice peut être définie comme l'échelle de répercussion du risque dans le corps social. Cette ampleur est notamment prise en compte par l'AI Act pour évaluer le risque de préjudice conditionnant la qualification de SIA à haut risque (AI Act, art. 7, §2, f).

Trois niveaux d'ampleur peuvent être définis :

Individuelle :

Ne concernant qu'un groupe restreint de personnes physiques et morales.

Sectorielle :

Affectant des pans limités mais importants de la vie sociale, ayant des conséquences pour des grands groupes de personnes physiques et morales (à une échelle géographique ou à l'échelle d'un secteur d'activité de la vie sociale ou économique).

Systémique :

Ayant des répercussions pour l'ensemble de la société et affectant les fondements même de la vie sociale.

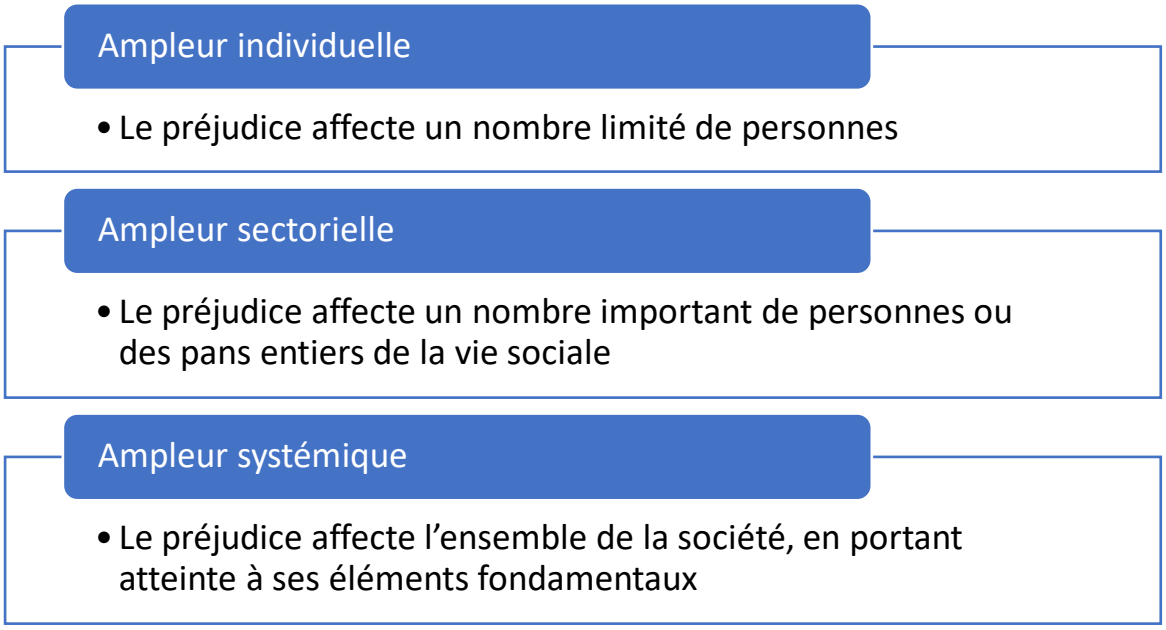
L'AI Act définit le risque systémique comme « un risque spécifique aux capacités à fort impact des modèles d'IA à usage général, ayant une incidence significative sur le marché de l'Union en raison de leur portée ou d'effets négatifs réels ou raisonnablement prévisibles sur la santé publique, la sûreté, la sécurité publique, les droits fondamentaux ou la société dans son ensemble, pouvant être propagé à grande échelle tout au long de la chaîne de valeur » (AI Act, art. 2, §65). Le considérant 110 de l'AI Act cite en outre les processus démocratiques, la sécurité économique et la diffusion de contenus illicites, faux ou discriminatoires. Il est possible de faire un rapprochement avec le *Digital services act* du 19 octobre 2022[159] (ci-après DSA) qui considère que sont des risques systémiques concernant les plateformes et les moteurs de recherche en ligne la diffusion de contenus illicites, les effets négatifs pour l'exercice des droits fondamentaux, les effets négatifs sur le discours civique, les processus électoraux et la sécurité publique et les effets négatifs lié aux violences sexistes et à la protection de la santé publique et des mineurs et les conséquences négatives graves sur le bien-être physique et mental des personnes (DSA, art. 34).

Ainsi, au sens de l'AI Act, le risque systémique peut être défini, d'une part, en tant que préjudice ayant une incidence significative sur le marché de l'Union en raison de sa portée et, d'autre part, comme un préjudice particulier se propageant à grande échelle. Concernant le premier aspect de la définition, l'annexe XIII de l'AI Act indique qu'un modèle d'IA[160] est présumé avoir un impact important sur le marché intérieur en raison de sa portée, lorsqu'il a été mis à la disposition d'au moins 10 000 utilisateurs professionnels enregistrés établis dans l'Union. Pour ce qui est du second aspect de la définition, il s'agit de prendre en compte l'ampleur d'un des préjudices cités. Plus précisément, le préjudice doit se propager à « grande échelle ». Ce concept n'est pas défini par l'AI Act mais le RGPD emploie ce terme ; il est donc possible de se référer, par analogie, aux décisions des autorités de contrôle y afférant. Selon les lignes directrices du G29, pour déterminer si un traitement est à grande échelle, il faut prendre en compte le nombre de personnes concernées, soit en valeur absolue, soit en valeur relative par rapport à la population concernée ; le volume de données et/ou le spectre des données traitées ; la durée, ou la permanence, des activités de traitement des données ; l'étendue géographique de l'activité de traitement[161]. Dans le contexte du fonctionnement du SIA, il faut également évoquer le concept d' « infraction de grande ampleur », défini par l'article 3, §61 de l'AI Act comme « tout acte ou toute omission contraire au droit de l'Union en matière de protection des intérêts des personnes, qui :

a) a porté ou est susceptible de porter atteinte aux intérêts collectifs des personnes résidant dans au moins deux États membres autres que celui : i) où l'acte ou l'omission en question a son origine ou a eu lieu ; ii) où le fournisseur concerné ou, le cas échéant, son mandataire, est situé ou établi ; ou iii) où le déployeur est établi, lorsque l'infraction est commise par le déployeur ;

b) a porté, porte ou est susceptible de porter atteinte aux intérêts collectifs des personnes, qui présente des caractéristiques communes, notamment la même pratique illégale ou la violation du même intérêt, et qui se produit simultanément, commise par le même opérateur, dans au moins trois États membres ».

En conclusion, il serait ainsi possible pour déterminer si le préjudice est susceptible de se propager à grande échelle de retenir, par analogie, les critères relatifs au nombre de personnes concernées, la durée ou la permanence du fonctionnement du SIA et l'étendue géographique de déploiement du SIA.



103. Les critères de détermination de l'ampleur. Pour déterminer précisément l'ampleur du préjudice, plusieurs critères peuvent être mobilisés.

En premier lieu, il faut prendre en considération le nombre de personnes physiques ou morales susceptibles de subir les conséquences du risque : quelques centaines de personnes ou des milliers ? Plus le nombre de personnes ou d'entreprises potentiellement concernées est grand, plus l'ampleur est possiblement grande. Comme il l'a été dit précédemment, ce critère est particulièrement pertinent pour déterminer si le risque est systémique.

En second lieu, l'ampleur dépend de la criticité du secteur concernée. Si le risque de préjudice pèse sur un secteur critique, alors il existe des indices importants permettant de dire que l'ampleur est sectorielle voire systémique. Pour définir ces secteurs critiques, on peut se référer à la liste des services essentiels définis par la directive 2022/2555 du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive SRI 2 ou NIS 2)[162], texte auquel l'AI Act fait référence (AI Act, art. 2, §62). Il s'agit de : l'énergie, comprenant l'électricité, les réseaux de chaleur et de froid, le pétrole, le gaz et l'hydrogène ; les transports, comprenant les transports aériens, ferroviaires, par eau et routiers ; le secteur bancaire ; les infrastructures de marchés financiers ; la santé ; l'eau potable ; les eaux usées ; l'infrastructure numérique ; la gestion des services TIC (interentreprises) ; l'administration publique ; et l'espace.

La combinaison d'un nombre très important de personnes (plusieurs millions de personnes) et d'un secteur critique permet de déterminer que l'ampleur du préjudice est systémique. Si le secteur est critique mais que le nombre de victimes potentielles est limité, alors l'ampleur sera plutôt sectorielle.

Référence Fiche-Risques VUE :

8) Quel est le nombre de personnes concernées ?

L'importance du nombre de victimes potentielles doit être évaluée en tenant compte des modalités prévues de déploiement du SIA (nombre de personnes affectées par le SIA ; conditions géographiques de déploiement ; durée prévue de déploiement).

9) Quelle est la criticité du secteur ?

Il faut indiquer si le secteur est critique ou non au sens de la directive NIS 2 précitée.

En fonction de ces critères, il est possible de définir le niveau d'ampleur parmi les trois précités :

Ampleur	Niveau
Individuelle	1
Sectorielle	2
Systémique	3

- L'évaluation de la sévérité des risques VUE

104. La combinaison des facteurs « conséquences » et « ampleur ». Pour évaluer le niveau de sévérité, c'est-à-dire pour déterminer si elle est faible, modérée ou importante, il convient d'associer les conséquences et l'ampleur du préjudice éventuel selon le produit suivant : conséquences*ampleur=sévérité.

Ainsi, le niveau de sévérité peut varier sur une échelle allant de 1, sévérité faible, à 9, sévérité importante :

Conséquences*Ampleur	Niveau de gravité
1 ou 2	Faible/1
3 ou 4	Modérée/2
6 ou 9	Importante/3

- La probabilité du préjudice :

105. Le facteur de la probabilité du préjudice. Le critère de la probabilité du préjudice n'est pas non plus défini par l'AI Act. On peut là encore se référer à la notion de probabilité au sens du RGPD. Selon la Cnil, la probabilité, ou vraisemblance du risque, « traduit la possibilité qu'un risque se réalise »[163]. Elle est négligeable lorsque « il ne semble pas possible que les sources de risques retenues puissent réaliser la menace en s'appuyant sur les caractéristiques des supports » ; limitée lorsque « il semble difficile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports » ; importante lorsque « il semble possible pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports » ; et maximale lorsque « il semble extrêmement facile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports »[164].

La Cnil s'appuie principalement sur les caractéristiques techniques des supports des données à caractère personnel. Transposé au contexte de l'IA, il convient ainsi de prendre en compte les caractéristiques techniques des SIA pour apprécier les probabilités de survenance du préjudice. A ce titre, on peut utilement se référer aux exigences imposées par l'AI Act en matière d'exactitude, de robustesse, de résilience et de cybersécurité. Néanmoins, les caractéristiques techniques d'un SIA ne sont que l'un des aspects de l'IA de confiance telle que définie par le Groupe d'experts de haut niveau sur l'IA indépendant constitué par la Commission européenne. Il convient de prendre d'autres éléments comme l'action humaine et contrôle humain, le respect de la vie privée et la gouvernance des données ou encore la transparence (AI Act, cons. 27). Il y a donc deux composantes à prendre en compte dans l'étude de la probabilité : les caractéristiques techniques de l'IA de confiance et des caractéristiques qu'on pourrait qualifier de « socio-techniques »[165].

106. Les caractéristiques techniques du SIA et la probabilité de survenance du préjudice. Les exigences relatives aux caractéristiques techniques des SIA sont régies par l'article 15 de l'AI Act. Il s'agit d'une exigence essentiel de l'AI Act imposant aux fournisseurs un certain nombre de vérifications. Ces exigences doivent être respectées dans le cadre général du système de gestion de risque applicable aux fournisseurs de SIA à haut risque. Ces caractéristiques sont les suivantes : l'exactitude, la robustesse, la résilience et la cybersécurité.

D'une manière générale, l'exactitude peut être définie comme la proximité entre les résultats du système observés et les résultats considérés comme vrais[166], la robustesse comme la capacité d'un système de maintenir son niveau de performance quelque soient les circonstances[167], la résilience comme la capacité du système de maintenir ses fonctions et sa structure malgré les changements internes et externes et de pouvoir fonctionner en mode « dégradé »[168] et la cybersécurité consiste en la capacité du système de résister aux actes intentionnels non-autorisés destinés à l'endommager[169]. Lorsque l'exactitude, la robustesse, la résilience ou la cybersécurité d'un SIA sont de faible niveau, la probabilité de survenance d'un préjudice est plus élevée que si ces caractéristiques sont d'un haut niveau.

Les niveaux d'exactitude, de robustesse, de résilience et de cybersécurité doivent être mesurés non seulement dans des conditions normales d'utilisation du SIA mais aussi dans le contexte des mauvaises utilisations raisonnablement prévisibles.

107. Les caractéristiques socio-techniques du SIA et la probabilité de survenance du préjudice. L'AI Act prévoit des exigences essentielles relatives à d'autres éléments que les caractéristiques techniques pouvant utilement limiter la probabilité de survenance du préjudice. Il s'agit des exigences suivantes :

Données et gouvernance des données (AI Act, article 10) :

L'article 10 de l'AI Act pose des exigences relatives aux données et à la gouvernance des données. Les données sont des éléments essentiels du fonctionnement des SIA et peuvent être la source des atteintes portées aux VUE. En effet, dans la mesure où les données d'entraînement, de validation et de test sont à la base du fonctionnement futur du SIA, elles ont une influence déterminante sur le risque que survienne un préjudice lors de l'utilisation du SIA. Par exemple, l'élimination de biais pouvant refléter des discriminations systémiques dans ces jeux de données permet d'éviter de reproduire ces discriminations lors de l'utilisation du SIA. Mais encore, la conception du SIA sur la base de données inadaptées au regard de la destination du SIA implique un risque accru d'erreurs du SIA lors de son utilisation.

Le paragraphe 2 relatif aux jeux de données d'entraînement, de validation et de test indique que ces jeux de données doivent être soumis à des pratiques en matière de gouvernance et de gestion des données appropriées à la destination du SIA, qu'il convient de respecter.

Le paragraphe 3 impose que les jeux de données d'entraînement, de validation et de test soient « pertinents, suffisamment représentatifs et, dans toute la mesure possible, exempts d'erreurs et complets au regard de la destination ». Ces jeux de données doivent posséder « les propriétés statistiques appropriées, y compris, le cas échéant, en ce qui concerne les personnes ou groupes de personnes à l'égard desquels le système d'IA à haut risque est destiné à être utilisé ».

Puis, le paragraphe 4 énonce que les jeux de données doivent tenir « compte, dans la mesure requise par la destination, des caractéristiques ou éléments propres au cadre géographique, contextuel, comportemental ou fonctionnel spécifique dans lequel le système d'IA à haut risque est destiné à être utilisé ».

Transparence et fourniture d'informations aux déployeurs (AI Act, article 13) :

Dans certains domaines, la transparence est présentée par l'AI Act comme un moyen de garantir le respect des droits fondamentaux et des VUE (AI Act, cons. 59, 60 et 66). Il s'agit notamment d'informer le déployeur sur toutes circonstances connues ou prévisibles liées à l'utilisation du système d'IA à haut risque conformément à sa destination ou dans des conditions de mauvaise utilisation raisonnablement prévisible, susceptibles d'entraîner des risques pour la santé et la sécurité ou pour les droits fondamentaux » (AI Act, art. 13, §3, sous b, sous iii). Cette information pourrait consister à fournir à l'utilisateur une version simplifiée et résumée de l'étude d'impact sur les VUE présentant les risques et les mesures de gestion des risques adoptées ou préconisées par le fournisseur, permettant ainsi de réduire la probabilité qu'un évènement préjudiciable prévisible se produise.

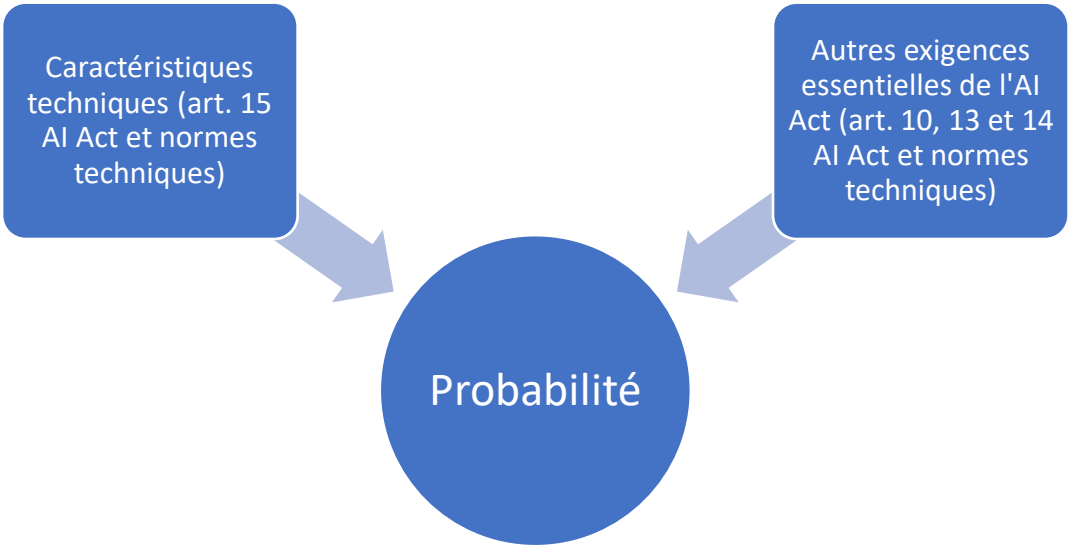
On peut également considérer comme particulièrement importantes pour limiter la probabilité de survenance du préjudice les informations relatives à :

- la destination du SIA (AI Act, art. 13, §3, b, i) ;
- le niveau d'exactitude, (AI Act, art. 13, §3, b, ii) ;
- la performance du SIA en ce qui concerne des personnes ou groupes de personnes spécifiques à l'égard desquels le système est destiné à être utilisé (AI Act, art. 13, §3, b, v) ;
- et les ressources informatiques et matérielles nécessaires, la durée de vie attendue du SIA et toutes les mesures de maintenance et de suivi, y compris leur fréquence, nécessaires pour assurer le bon fonctionnement du SIA, notamment en ce qui concerne les mises à jour logicielles (AI Act, art. 13, §3, e).

Contrôle humain (AI Act, article 14) :

L'article 14 de l'AI Act prévoit des exigences liées au contrôle humain[170]. Il s'agit d'une exigence importante pour le respect des VUE. En effet, le paragraphe 2 indique que « le contrôle humain vise à prévenir ou à réduire au minimum les risques pour la santé, la sécurité ou les droits fondamentaux ». Le contrôle humain est expressément présenté comme un moyen permettant de garantir la protection des droits fondamentaux et en conséquence les VUE. Il peut notamment permettre de limiter la probabilité de survenance de certains préjudices, notamment des préjudices liés à un défaut d'exactitude du SIA.

108. L'importance des normes techniques et spécifications communes. Enfin, il est essentiel de prendre en compte les normes techniques applicables aux SIA, qu'il s'agisse de norme horizontale (applicables à tous les SIA quel que soit leur destination) ou verticale (visant des destinations/secteurs spécifiques). Les propriétés techniques des SIA prévues par ces normes peuvent avoir pour objectif de réduire la probabilité de survenance de préjudices et devraient, à ce titre, être mises en œuvre. Notons que le respect de normes harmonisées[171] ou de spécifications communes[172] élaborées dans le contexte de l'AI Act permet de bénéficier d'une présomption de conformité aux exigences essentielles de la section 2 du chapitre III de l'AI Act (AI Act, art. 40 et 41).



Référence Fiche-Risques VUE :

10) Quel est le niveau d'exactitude du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau d'exactitude est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ?

Il doit être fait au référence au niveau d'exactitude attendu du SIA dans des conditions normales d'utilisation, c'est-à-dire conformément à sa destination et tel qu'il ressort des test effectués, et dans des conditions de mauvaise utilisation raisonnablement prévisibles selon les métriques définies par les normes techniques applicables au SIA.

Il convient également de mentionner de quelle façon l'exactitude garantit la performance du système et son influence sur la probabilité de survenance du préjudice.

11) Quel est le niveau de robustesse du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de robustesse est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ?

La robustesse du SIA doit être décrite et détaillée selon les normes techniques applicables. Il convient de préciser les conséquences du niveau de robustesse sur la probabilité de survenance du préjudice.

12) Quel est le niveau de résilience du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de

résilience est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ?

La résilience du SIA doit être décrite et détaillée selon les normes techniques applicables. Il convient de détailler les éléments permettant de garantir la résilience du SIA. Il convient également d'indiquer de quelle façon la résilience du SIA a une influence sur la probabilité de survenance du préjudice.

13) Quel est le niveau de cybersécurité du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de cybersécurité est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ?

La cybersécurité du SIA doit être décrite et détaillée selon les normes techniques applicables. Il convient de préciser de quelle façon les mesures de cybersécurité ont une influence sur la probabilité de survenance du préjudice.

14) Les jeux de données d'entraînement, de validation et de test font-ils l'objet de pratiques de gouvernance et de gestion des données conformes aux dispositions de l'article 10, §2 de l'AI Act ?

Il convient de démonter la conformité des pratiques de gouvernance et de gestion des données des jeux de données précités aux dispositions de l'article 10 de l'AI Act et aux normes techniques applicables et comment ces pratiques de gouvernance et de gestion des données permettent de réduire la probabilité de survenance du préjudice.

15) Les jeux de données d'entraînement, de validation et de test sont-ils pertinents, suffisamment représentatifs et, dans toute la mesure possible, exempts d'erreurs et complets au regard de la destination, conformément aux dispositions de l'article 10, §3 de l'AI Act ? Présentent-ils les propriétés statistiques appropriées, y compris, le cas échéant, en ce qui concerne les personnes ou groupes de personnes à l'égard desquels le SIA est destiné à être utilisé, conformément aux dispositions de l'article 10, §3 de l'AI Act ?

Il faut démontrer la pertinence, la représentativité, l'absence d'erreur et la complétude des jeux de données précités ainsi que le caractère approprié de leurs propriétés statistiques. Il convient de faire référence aux normes techniques applicables et d'expliquer comment les caractéristiques des jeux de données ont une influence sur la probabilité de survenance du préjudice.

16) Les jeux de données d'entraînement, de validation et de test tiennent-ils compte, dans la mesure requise par la destination, des caractéristiques ou éléments propres au cadre géographique, contextuel, comportemental ou fonctionnel spécifique dans lequel le SIA est destiné à être utilisé, conformément aux dispositions de l'article 10, §4 de l'AI Act ?

Il faut démonter comment, conformément aux dispositions de l'article 10 de l'AI Act, les jeux de données prennent en compte le contexte de déploiement du SIA et de quelle façon cela influence la probabilité de survenance du préjudice.

17) Est-il prévu de mentionner dans la notice d'utilisation les informations suivantes, conformément aux dispositions de l'article 13 de l'AI Act : - la destination du SIA ; - le niveau d'exactitude, y compris les indicateurs utilisés, de robustesse et de cybersécurité qui a servi de référence pour les tests et la validation du SIA et qui peut être attendu, ainsi que toutes circonstances connues et prévisibles susceptibles d'avoir une incidence sur le niveau attendu d'exactitude, de robustesse et de cybersécurité ; - le cas échéant, la performance du SIA en ce

qui concerne des personnes ou groupes de personnes spécifiques à l'égard desquels le système est destiné à être utilisé ; - et les ressources informatiques et matérielles nécessaires, la durée de vie attendue du SIA et toutes les mesures de maintenance et de suivi, y compris leur fréquence, nécessaires pour assurer le bon fonctionnement du SIA, notamment en ce qui concerne les mises à jour logicielles ?

Il convient de préciser comment et de quelle façon ces informations seront portées à la connaissance des personnes intéressées, notamment les déployeurs.

18) Quelles sont les mesures de contrôle humain mises en place, conformément aux dispositions de l'article 14 de l'AI Act ? De quelle façon permettent-elles de réduire la probabilité de survenance du préjudice ?

Il convient de décrire les mesures de contrôle humain prévues et de justifier la pertinence de ces mesures en vue de la réduction de la probabilité de survenance du préjudice et l'influence qu'elles ont sur la probabilité.

Sur la base de ces deux éléments, il convient de déterminer la probabilité de survenance du préjudice, selon l'échelle suivante :

Probabilité	Niveau
Faible	1
Modérée	2
Importante	3

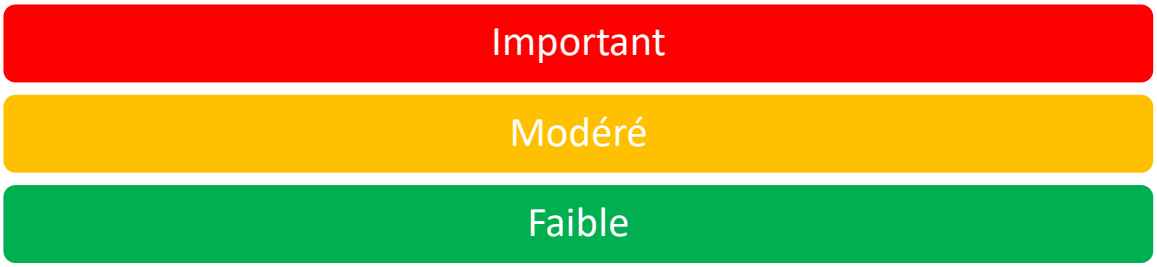
- La détermination du niveau de risque :

109. Les différents niveaux de risques et leurs conséquences. Le niveau de risque reflète l'importance du risque d'atteinte aux VUE et son acceptation au regard du contrôle de proportionnalité qui sera réalisé lors de la phase suivante.

On peut retenir trois niveaux de risque[173] : le risque faible ; modéré ; important. Un risque faible signifie que la potentialité d'atteinte aux VUE est peu probable ou que la sévérité du préjudice est minime et dans ce cas on peut tenir le risque comme nul ; un risque modéré que le préjudice est possible ou que sa sévérité n'est pas significative, un risque important que le risque de préjudice est certain ou que sa sévérité est considérable.

L'identification d'un risque faible n'impliquera aucun changement dans la conception du SIA puisqu'on le considère comme étant nul. En revanche, lorsque le risque est modéré, il peut convenir, après avoir réalisé le contrôle de proportionnalité, d'adopter des mesures de gestion des risques pour réduire le niveau de risque. Enfin, lorsque le risque est important, il est très probable que le contrôle de proportionnalité révèle une disproportion rendant nécessaire l'adoption de mesures de gestion des risques.

NIVEAUX DE RISQUE



110. La détermination du niveau de risque. Comme indiqué précédemment, le niveau de risque au sein de l'AI Act est apprécié au regard de la sévérité et de la probabilité du préjudice. L'évaluation du niveau de risque consiste donc à combiner ces deux facteurs : sévérité du préjudice*probabilité du préjudice = niveau de risque. On peut ainsi obtenir un score de risque compris entre 1 et 9, 1 correspondant au niveau le plus faible et 9 à une importance maximale.

Score	Niveau de risque
1 ou 2	Faible
3 ou 4	Modéré
6 ou 9	Important

111. Le résultat de la combinaison des facteurs « sévérité » et « probabilité ». Une fois que les niveaux de sévérité et de probabilité du préjudice sont définis, il est possible de déterminer le niveau de risque en se reportant au tableau suivant.

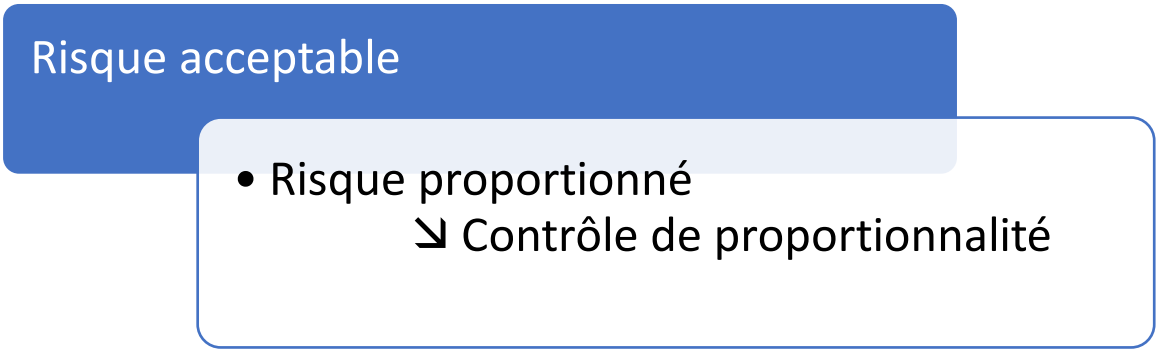
		Probabilité		
		1	2	3
Sévérité	1	1	2	3
	2	2	4	6
	3	3	6	9

Le niveau de risque ainsi obtenu devra ensuite être indiqué dans la *Fiche-Risques VUE* et dans le *Tableau synthétique de l'étude d'impact*.

ii. Évaluer la proportionnalité du risque VUE

112. La proportionnalité et l'acceptabilité du risque. L'AI Act n'exige pas que les SIA ne présentent aucun risque mais que les risques, s'il y en a, soient acceptables[174]. L'acceptabilité du risque découle de sa proportionnalité aux autres intérêts que le SIA met en œuvre. En cas de disproportion entre le risque d'atteinte aux VUE et les intérêts mis en œuvre par le SIA, le risque doit être considéré comme étant inacceptable.

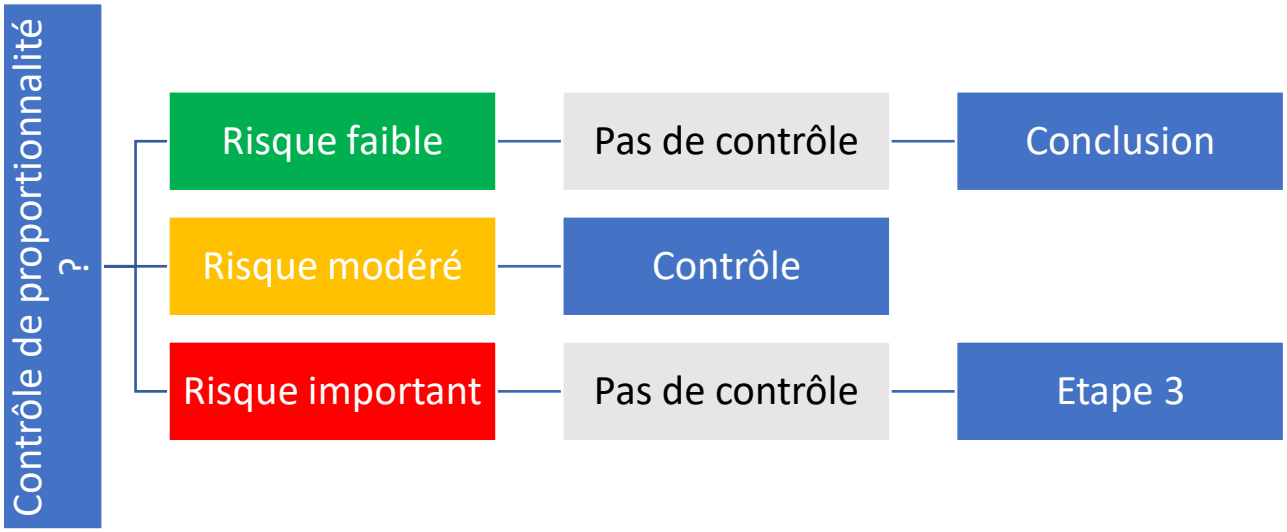
Pour établir que le risque est « acceptable », c'est-à-dire proportionné, il faut donc réaliser un contrôle de proportionnalité.



113. L'exigence de contrôle de la proportionnalité : un risque modéré. Le contrôle de proportionnalité devra uniquement être réalisé si le risque identifié est de niveau modéré.

Lorsque le risque est faible, on peut considérer que l'atteinte aux VUE n'est pas probable, soit parce que la probabilité est quasi-nulle, soit parce que la sévérité du préjudice n'est pas suffisamment grave pour pouvoir considérer qu'il y a un risque d'atteinte au « bon fonctionnement des sociétés européennes ». Néanmoins, il convient de garder à l'esprit que l'atteinte aux VUE doit être distinguée de l'atteinte aux droits fondamentaux des personnes et que même s'il n'y a pas de risque d'atteinte aux VUE, une atteinte aux droits fondamentaux dans des cas individuels demeure possible ; celle-ci devrait être appréhendée et traitée par le système général de gestion des risques du fournisseur (AI Act, art 9 préc.). En cas de risque faible, il n'est donc pas nécessaire de prendre de mesure de gestion du risque faible d'atteinte aux VUE et il faut se reporter directement à la conclusion de l'étude d'impact.

A l'inverse, lorsque le risque est important, on peut présumer de l'atteinte aux VUE. Le contrôle de la proportionnalité n'est pas nécessaire car le niveau de risque est tel qu'il n'est pas acceptable. Dans ce cas, il faut se reporter directement à l'étape 3 relative à la gestion des risques.

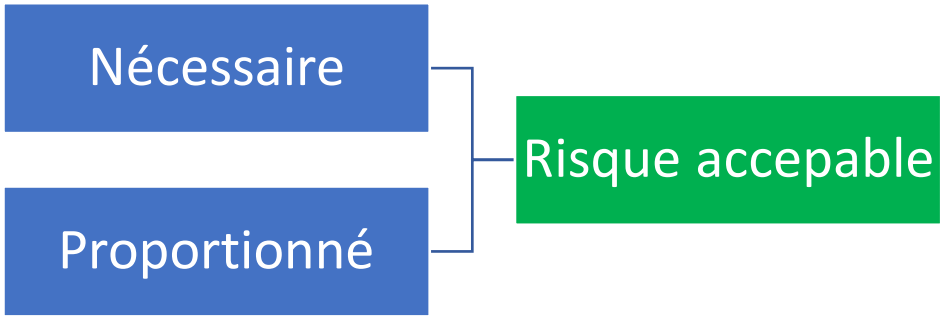


114. Le contrôle de la proportionnalité : présentation. Le contrôle de proportionnalité consiste à vérifier que le risque d'atteinte aux VUE du fait de l'utilisation du SIA. Le contrôle de proportionnalité est une méthode de raisonnement du juge consistant à mettre en balance des principes juridiques de rang équivalent, simultanément applicables mais antinomiques[175]. Ce contrôle s'appuie en principe sur trois critères : approprié, nécessaire et proportionné[176].

En pratique, il n'y a pas de modèle unique ou dominant de raisonnement mis en œuvre par la CJUE en matière de proportionnalité[177] :

« En fonction du contentieux, la Cour peut ne pas viser certaines des trois exigences : le caractère approprié de la mesure peut aller de soi et, partant, ne pas mériter de développements particuliers ; la démonstration de la proportionnalité peut passer par celle de la nécessité »[178].

Concernant le contrôle de la proportionné de la mise en œuvre d'un SIA dans un contexte de risque pour les VUE, on peut considérer que le caractère approprié sera le plus souvent tenu pour acquis. En effet, la recherche du caractère approprié consisterait à déterminer si la destination du SIA est adéquate au regard des finalités poursuivies par le déployeur et si la performance du SIA est satisfaisante pour atteindre les finalités poursuivies. On peut présumer que ce sera généralement le cas, un déployeur n'ayant pas d'intérêt à utiliser un SIA n'ayant pas de lien avec les finalités qu'il poursuit ou qui ne serait pas suffisamment performant. En revanche, il convient de retenir les critères de la nécessité et de la proportionnalité *stricto sensu*[179]. Ces deux conditions supposent une étude approfondie car leur satisfaction est moins évidente, notamment parce qu'il s'agit de prendre en compte d'autres éléments que les seules finalités poursuivies par le déployeur.



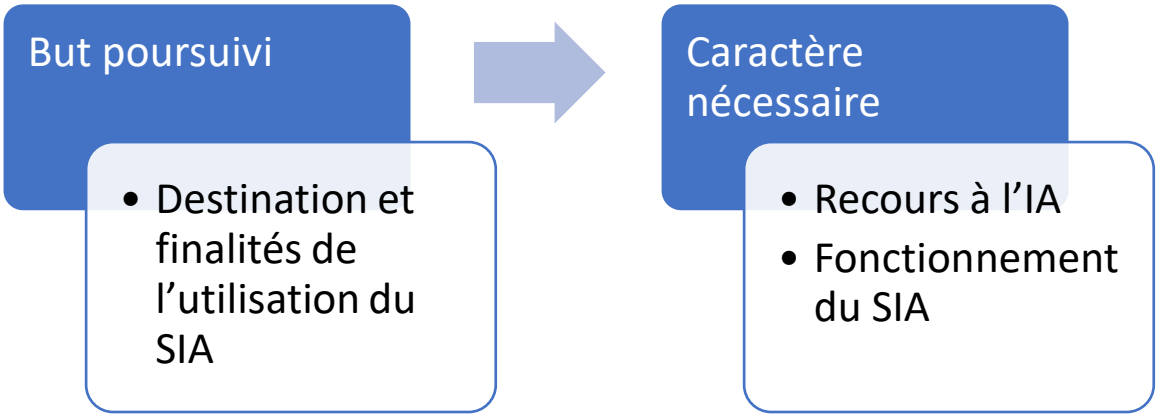
115. La mise en œuvre du contrôle de la proportionnalité. La mise en œuvre du contrôle de la proportionnalité doit s'appuyer sur la description du SIA. Plus précisément, pour chacun des éléments permettant de réaliser le contrôle de proportionnalité :

Nécessaire	Proportionné
• Destination ou finalités de l'utilisation du SIA (ques. 2 Tableau descriptif) • Tâches peuvent être réalisées sans le SIA (ques. 5 Tableau descriptif) • Avantages du recours au SIA (ques. 6 Tableau descriptif) • Caractéristiques du SIA (ques. 12 et s. Tableau descriptif)	• Destination et finalités de l'utilisation du SIA (ques. 2 Tableau descriptif) • Nature de l'intérêt poursuivi

116. Le contrôle de la proportionnalité : le caractère nécessaire. En premier lieu, l'utilisation du SIA doit être nécessaire, c'est-à-dire que l'utilisation du SIA ne doit pas excéder ce qu'exige la réalisation du but poursuivi et cet objectif ne doit pas pouvoir être atteint par des moyens moins attentatoires aux VUE. Si d'autres moyens plus respectueux des VUE sont adaptés, l'utilisation du SIA, telle qu'initialement prévue, ne peut pas être considérée comme nécessaire. Par analogie, le principe de la nécessité peut être comparé au principe de minimisation prévu par l'article 5 du RGPD selon lequel les données à caractère personnel traitées doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ».

Pour déterminer si l'atteinte aux VUE est nécessaire, il faut établir, au regard des finalités poursuivies par le déployeur si :

- d'une part, l'utilisation d'un dispositif recourant à des technologies d'IA apporte une plus-value par rapport à des dispositifs n'utilisant pas l'IA, c'est-à-dire si le but recherché peut être réalisé tout aussi efficacement sans recours à l'IA et ;
- d'autre part, les conditions de mise en œuvre du SIA au regard des technologies utilisées ou du contexte dans lequel il est déployé et son échelle d'utilisation n'outrepassent pas ce qui peut être suffisant pour atteindre la destination ou les finalités du SIA.



Référence Fiche-Risques VUE :

20) Le recours aux technologies d'IA offre-t-il des avantages significatifs ? Indiquez précisément pour chaque fonction du SIA la plus-value qu'apporte l'IA

Il convient de justifier les intérêts du recours à l'IA. Ce peut être soit parce que la tâche considérée ne peut pas être raisonnablement réalisé par sans utilisation de l'IA (par un système automatisé sans IA ou par un humain) soit parce que l'utilisation de l'IA permet de réaliser les tâches plus efficacement (par exemple plus rapidement ou avec plus de précision). Il est possible par exemple de se référencer au système HABA-MABA.

21) Les conditions de déploiement du SIA (lieux et plages horaires d'utilisation) sont-elles nécessaires pour la mise en œuvre de la destination ou de la finalité poursuivie ? Justifiez ce caractère nécessaire

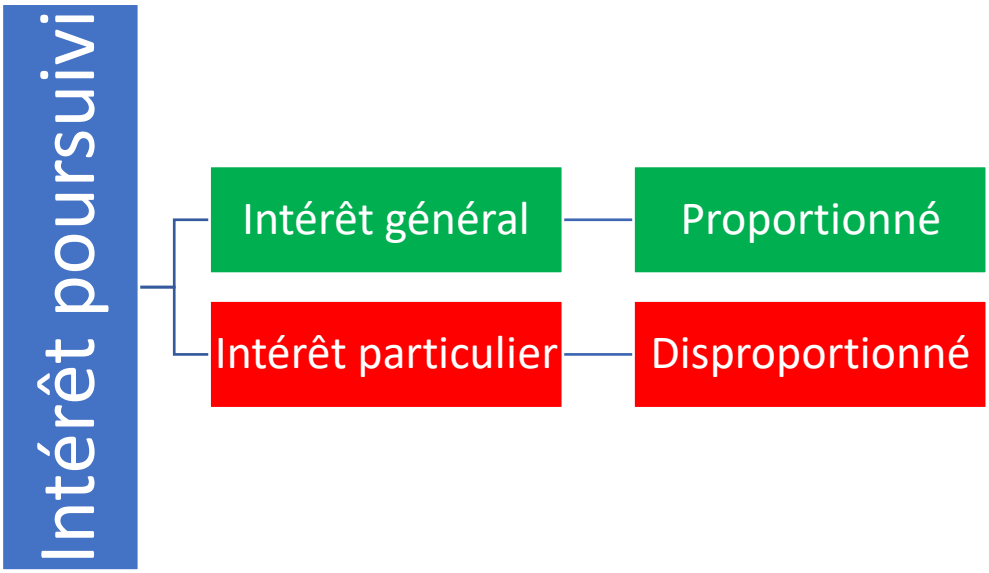
Il convient de justifier les conditions de déploiement par rapport à la destination ou à la finalité de l'utilisation du SIA. Ces conditions de déploiement doivent être strictement suffisantes et nécessaires, elles ne doivent pas être excessives. Ainsi, par exemple, si le SIA est utilisé pour assurer la sécurité de lieux accueillant un nombre important de personnes, il convient de s'assurer que les modalités de déploiement sont cantonnées à des contextes correspondant à cette destination ou finalité (c'est-à-dire dans des lieux et à des horaires connaissant un flux important de personnes).

22) L'échelle d'utilisation du SIA est-elle nécessaire pour la mise en œuvre de la destination ou de la finalité poursuivie ? Justifiez ce caractère nécessaire

L'échelle d'utilisation du SIA doit correspondre à ce qui est nécessaire au regard de la destination du SIA ou de la finalité poursuivie par le déployeur. Ainsi, par exemple, si le SIA répond à un besoin précis limité dans le temps, un déploiement pour une durée indéterminé peut être excessive et non-nécessaire.

117. Le contrôle de la proportionnalité : le caractère proportionné *stricto sensu*. En second lieu, l'atteinte doit être proportionnée. Il s'agit de la proportionnalité *stricto sensu*. Établir la proportionnalité de l'atteinte consiste à déterminer si la destination du SIA ou les finalités poursuivies par le déployeur sont compatibles avec les VUE, c'est-à-dire que l'atteinte aux VUE n'est pas démesurée par rapport aux avantages qu'il y a à atteindre les finalités. Il s'agit de mettre en balance les intérêts que le SIA cherche à satisfaire avec les risques d'atteinte aux VUE. Les risques doivent être proportionnés à ces intérêts. Ainsi, plus le risque est grand, plus l'intérêt poursuivi par la destination ou par le déployeur du SIA doit être important.

Plus précisément, concernant le sens à donner à la notion d'intérêt poursuivi par la destination du SIA ou le déployeur, il faut se demander si la destination ou les finalités poursuivies peuvent être rattachées à l'intérêt général et à la protection des droits et principes fondamentaux ou s'il ne s'agit que d'intérêts personnels. Pour cela, il est possible d'utiliser comme référence la Charte des droits fondamentaux de l'Union européenne, reproduite dans l'annexe 2. Si l'intérêt poursuivi par la destination ou le déployeur correspond à l'un des droits ou principes fondamentaux protégés par ce texte alors il s'agit d'un intérêt général et le niveau de risque est proportionné. En revanche, si l'intérêt poursuivi ne saurait y être rattaché, alors il faut considérer qu'il s'agit d'un intérêt particulier et le niveau de risque est disproportionné.



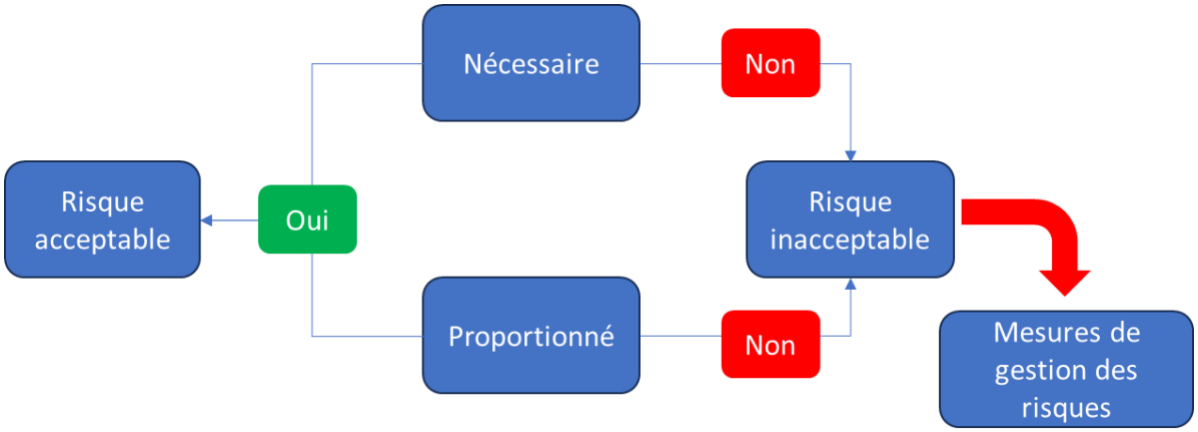
Référence Fiche-Risques VUE :

<u>24) Quelle est la nature des intérêts poursuivis par la destination ou par le déployeur du SIA et lesquels sont-ils ?</u>

Il convient d'indiquer la nature de l'intérêt poursuivi et d'indiquer de quel intérêt il s'agit précisément, notamment, si possible, par référence aux droits et principes fondamentaux de la Charte des droits fondamentaux de l'Union européenne.

118. Le résultat final du contrôle de la proportionnalité. La mise en œuvre du contrôle de la proportionnalité peut donner deux résultats :

- Soit le risque est proportionné car il l'utilisation du SIA est nécessaire et proportionnée *stricto sensu* :
  - Le risque est acceptable et aucune mesure de gestion des risques n'est nécessaire ;
- Soit le risque est disproportionné car l'utilisation du SIA n'est pas nécessaire ou n'est pas proportionnée *stricto sensu* :
  - Dans ce cas, le risque n'est pas acceptable et des mesures de gestion de risque permettant d'éliminer ou de réduire le niveau du risque doivent être instaurées.



Il convient d'indiquer dans le *Fiche-Risques VUE* et le *Tableau synthétique de l'étude d'impact* si le risque est ou n'est pas acceptable et pour quelles raisons. En effet, la motivation du résultat permet de prendre les mesures de gestion des risques adaptées pour rendre le risque acceptable.

3. Étape 3 : La gestion des risques : Fiche-Gestion risques VUE (annexe 6)

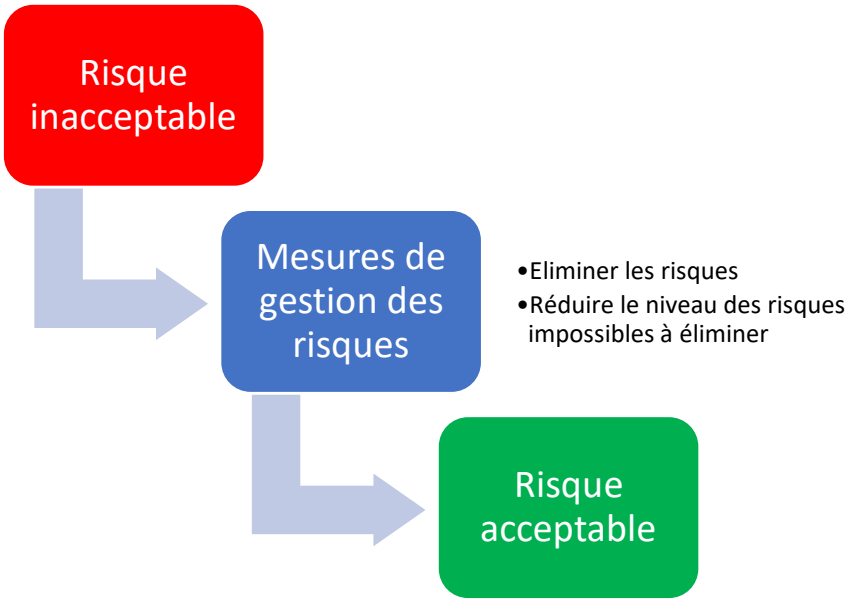
119. La troisième phase de l'étude d'impact : les mesures de gestion des risques. L'objectif de cette étape est d'éliminer ou de réduire le niveau des risques inacceptables identifiés lors de la phase précédente[180]. L'AI Act offre un cadre générique intéressant sur ce point dans le contexte du système de gestion des risques que les fournisseurs de SIA à haut risque doivent mettre en place (art. 9) au titre des exigences essentielles. L'étude d'impact sur les VUE peut donc s'en inspirer, étant rappelé que les risques faibles d'atteintes aux VUE sont exclus de la gestion des risques puisqu'ils sont considérés comme proportionnés[181].

a. Les objectifs et la nature des mesures de gestion des risques

120. L'objectif des mesures de gestion des risques : l'élimination ou la réduction du risque. L'élimination ou la réduction du niveau de risques est réalisée grâce à la mise en place de mesures de gestion des risques.

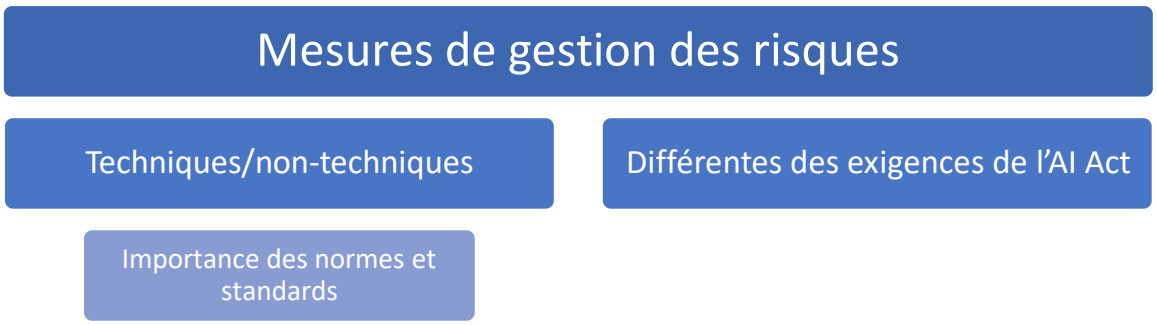
Selon l'AI Act, les mesures de gestion des risques dans le cadre du système de gestion des risques de l'article 9 ont pour objectif d'éliminer ou réduire les risques autant que la technologie le permet grâce à une conception et à un développement appropriés du SIA sauf si le risque s'avère impossible à éliminer, auquel cas les mesures doivent consister à « mettre en

œuvre […] des mesures adéquates d'atténuation et de contrôle » (AI Act, art. 9, §5, a et b). Plus précisément, les mesures de gestion des risques doivent permettre de rendre le risque « acceptable ». L'article 9, §5 de l'AI Act indique que les mesures de gestion des risques « sont telles que le risque résiduel pertinent associé à chaque danger ainsi que le risque résiduel global lié aux systèmes d'IA à haut risque sont jugés acceptables ». En effet, s'il faut prendre des mesures, c'est parce que le risque a été identifié comme étant disproportionné et donc inacceptable. Les mesures de gestion des risques sont ainsi destinées éliminer tout risque ou, de manière plus pragmatique, à réduire au maximum le niveau de risque pour qu'il soit proportionné et donc acceptable. Si le risque s'avère disproportionné (à l'aune du contrôle de proportionnalité évoqué dans la phase précédente), le SIA ne pourra en principe pas être mis en circulation sur le marché européen[182]. Il est possible de transposer cet acquis règlementaire à l'étude d'impact sur les VUE.



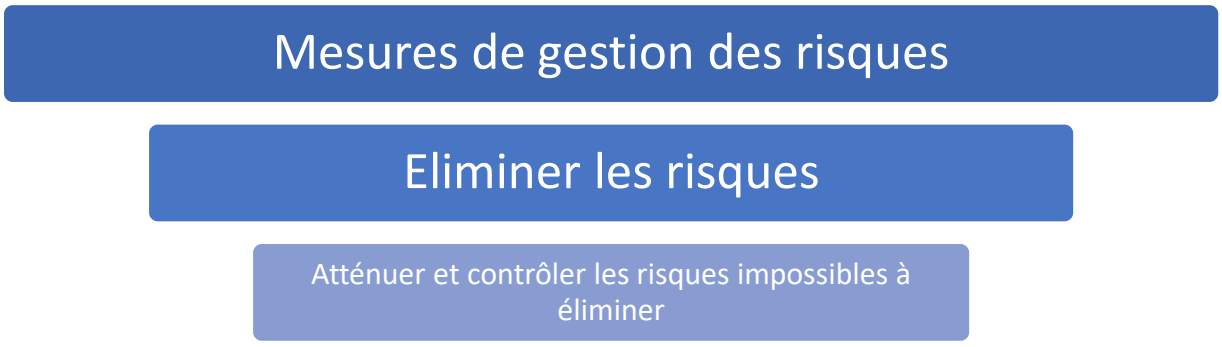
121. La nature des mesures de gestion des risques. Tout d'abord, les mesures de gestion des risques ne sont pas définies par l'AI Act mais il pourrait s'agir de mesures techniques, comme des mesures liées au fonctionnement du logiciel ou aux données, ou des mesures non-techniques, par exemple une gestion contractuelle des risques avec l'utilisateur[183]. Selon l'article 9, §3 de l'AI Act, les mesures de gestion des risques doivent prendre « en considération l'état de la technique généralement reconnu, notamment tel qu'il ressort des normes harmonisées ou des spécifications communes pertinentes ».

Ensuite, les mesures de gestion des risques doivent être distinguées des exigences essentielles prévues par les articles 10 et suivants de l'AI Act. L'article 9, §4 de l'AI Act en matière de système de gestion des risques indique en effet que lesdites mesures « tiennent dûment compte des effets et de l'interaction possibles résultant de l'application combinée des exigences énoncées dans la [section 2], en vue de prévenir les risques plus efficacement tout en parvenant à un bon équilibre dans le cadre de la mise en œuvre des mesures visant à répondre à ces exigences », à savoir les exigences des articles 10 et suivants. Les mesures de gestion des risques ont donc vocation à compléter ces exigences dans l'hypothèse où ces dernières ne permettraient pas de rendre le risque acceptable. Cet acquis générique en matière de système de gestion des risques peut utilement être transposé, par analogie, à l'étude d'impact VUE.



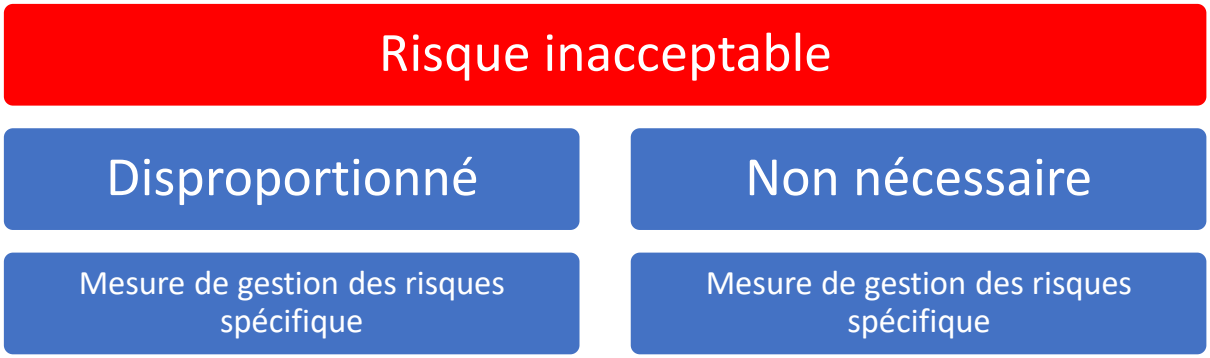
122. L'élimination ou la réduction du risque : définitions et enjeux. Les mesures de gestion des risques doivent avoir pour principal but l'élimination du risque. L'objectif à atteindre est l'absence de risque. Le premier objectif des mesures de gestion des risques est donc l'élimination du risque.

Toutefois, l'AI Act admet que certains risques sont « *impossibles à éliminer* » (AI Act, art. 9, §4, b). Le texte ne précise pas de quels risques il s'agit. On pourrait supposer qu'il s'agit de risques consubstantiels au fonctionnement du SIA, existants du fait même de la destination ou des fonctions et fonctionnements essentiels du SIA, impliquant que l'élimination de ces risques ne soit rendue possible que par l'absence de recours au SIA. Cette solution doit être envisagée en tant que mesure de dernier recours, si les risques résiduels ne peuvent pas être abaissés à un niveau acceptable. En effet, en cas d'impossibilité d'éliminer un risque, l'AI Act exige la mise en œuvre de « mesures adéquates d'atténuation et de contrôle » de ce risque. L'objectif de ces mesures d'atténuation et de contrôle, et plus largement des mesures de gestion des risques, est d'atteindre un niveau de risque acceptable. Si le risque résiduel impossible à éliminer peut-être réduit à un niveau acceptable, le SIA peut être mis sur le marché et utilisé. En revanche, si ce risque demeure inacceptable, il faut considérer la possibilité de ne pas mettre sur le marché ou mettre en service le SIA.

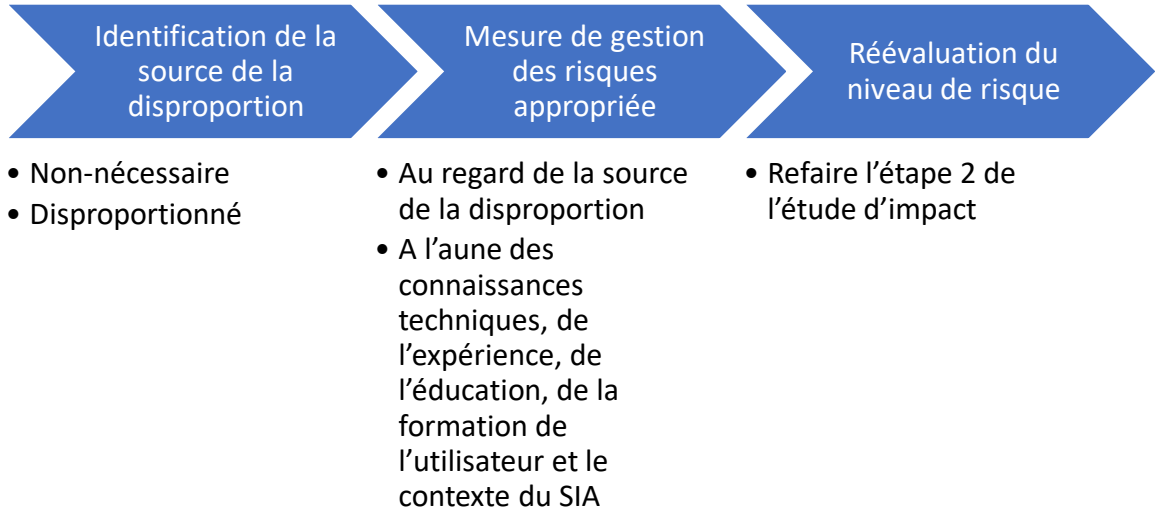


123. La méthode d'identification des mesures de gestion des risques adaptées : présentation. L'inacceptabilité du risque découle de sa disproportion. Les mesures de gestion des risques destinées à rendre le risque acceptable consiste donc à rétablir la proportionnalité du risque et de l'utilisation du SIA, c'est-à-dire son caractère nécessaire et proportionné.

Pour identifier les mesures de gestion des risques adaptées, il convient donc au préalable de déterminer l'origine de la disproportion, qui peut être l'absence du caractère nécessaire ou proportionné, en s'appuyant sur les résultats de l'étape précédente. Les mesures de gestion des risques doivent répondre spécifiquement à chacun des problèmes afin de permettre une élimination ou une réduction efficace du risque. Une mesure de gestion des risques spécifique peut toutefois permettre de résoudre plusieurs problèmes.



Après avoir défini les mesures de gestion de risques appropriées, il convient de réévaluer le niveau de risque. L'objectif à atteindre est un niveau de risque acceptable. Pour ce faire, il convient de réaliser une nouvelle étude d'impact prenant en compte les mesures de gestion de risques adoptées.



b. La détermination des mesures de gestion des risques appropriées

124. La méthode d'identification des mesures de gestion des risques appropriées. Plusieurs éléments doivent être pris en compte pour déterminer les mesures de gestion des risques appropriées. En premier lieu, il convient de prendre en compte la source de la disproportion. En second lieu, l'AI Act précise que pour « l'élimination ou de la réduction des risques liés à l'utilisation du système d'IA à haut risque, il est dûment tenu compte des connaissances techniques, de l'expérience, de l'éducation et de la formation pouvant être attendues du déployeur, ainsi que du contexte prévisible dans lequel le système est destiné à être utilisé » (AI Act, art. 9, §5). Cette prescription est également pertinente pour ce qui concerne l'élimination ou la réduction des risques pour les VUE.

125. Une réponse adaptée à la source de la disproportion. La mesure de gestion des risques à adopter ne sera pas la même selon la source de la disproportion. Il convient donc de distinguer les réponses à apporter en cas de caractère non-nécessaire ou disproportionné du SIA.

- Caractère non-nécessaire

La non-nécessité du SIA procède du fait :

- que la tâche assignée au SIA peut être réalisée par d'autres moyens n'ayant pas recours à l'IA de façon toute aussi efficace ;
- que cette tâche peut être effectuée par d'autres moyens n'ayant pas recours à l'IA ou selon d'autres modalités de fonctionnement du SIA moins attentatoires aux VUE tout en étant aussi efficace.

Pour répondre à ce problème, il convient d'adopter des mesures qui limitent le recours à l'IA pour certaines fonctionnalités très précises pour lesquelles le recours à l'IA est plus efficace que d'autres techniques ou des mesures permettant une mise en œuvre du SIA plus respectueuse des VUE.

Référence Fiche-Gestion risques VUE :

1) Les fonctions n'offrant pas d'avantages significatifs peuvent-elles être supprimées sans porter atteinte à la performance du SIA ni nuire à la possibilité pour le SIA d'atteindre la finalité poursuivie ?

Le SIA n'est pas nécessaire si le système n'est pas plus efficace qu'un fonctionnement sans IA. Il convient alors de supprimer ces fonctions si cela est possible, c'est-à-dire sans porter atteinte à la performance du SIA, définie comme la capacité du SIA à remplir sa destination (AI Act, art. 3, §18), ou à la possibilité de satisfaire les finalités de son utilisation par le déployeur.

S'il n'est pas possible de supprimer ces fonctions sans porter atteinte à la performance ou à la possibilité de satisfaire les finalités, il convient de repenser la conception et le développement du SIA.

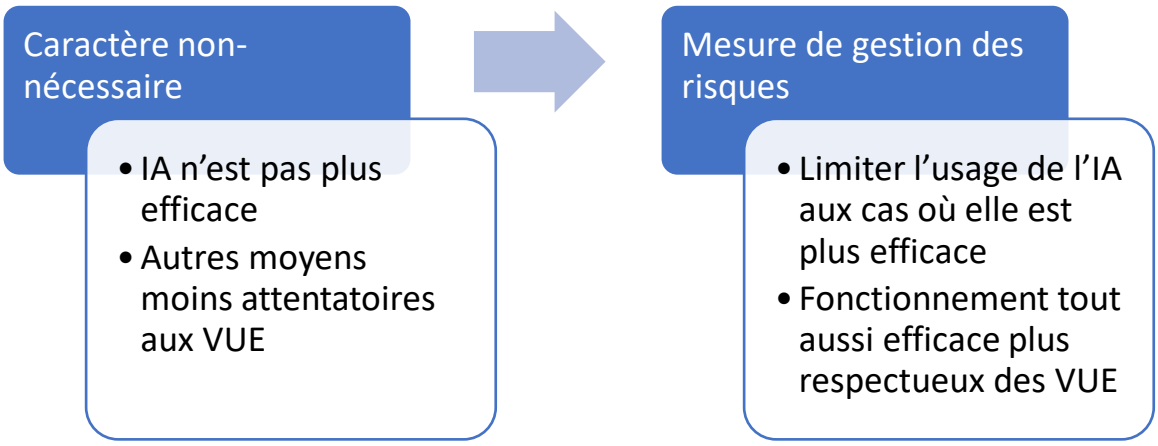
2) Les conditions de déploiement ont-elles été définies par rapport à la destination ou la finalité poursuivie ?

3) Est-il possible modifier les conditions de déploiement du SIA sans porter atteinte à la performance du SIA ou à la possibilité de réaliser la finalité poursuivie ?

Les conditions de déploiement doivent correspondre à ce qui est nécessaire au regard de la destination du SIA ou de la finalité poursuivie par le déployeur. S'il n'est pas possible de modifier les conditions de déploiement sans porter atteinte à la performance ou à la possibilité de satisfaire les finalités, il convient de repenser la conception et le développement du SIA.

4) L'échelle d'utilisation a-t-elle été déterminée au regard de la destination ou de la finalité poursuivie ?

L'échelle d'utilisation doit correspondre à ce qui est nécessaire au regard de la destination du SIA ou de la finalité poursuivie par le déployeur.



- Caractère disproportionné

Le caractère disproportionné résulte d'un déséquilibre entre les intérêts que le SIA met en œuvre et le risque d'atteinte aux VUE. Il convient dans cette hypothèse de prendre des mesures ayant pour finalité d'éliminer ou de réduire les risques que le SIA présente pour les VUE. Plus précisément, il va s'agir de chercher à diminuer les niveaux de sévérité ou de probabilité du préjudice.

Référence Fiche-Gestion risques VUE :

5) Le risque de préjudice peut-il être éliminé sans porter atteinte à la performance du SIA ou à la réalisation de la finalité poursuivie ?

Les mesures de gestion des risques ont pour premier objectif l'élimination des risques. Il faut donc chercher tout d'abord à éliminer le risque. Si cela n'est pas possible, au regard de la performance du SIA ou de la finalité poursuivie, alors il faut chercher à réduire le niveau de risque.

6) Quel niveau global de risque est visé ?

Pour atteindre la proportionnalité stricto sensu*, il convient de réduire le niveau de risque. Ainsi, si le risque était important, il convient de réduire le niveau de risque à un niveau modéré ou, idéalement faible. Si le risque était modéré, il convient d'atteindre un niveau de risque faible.*

7) Pour réaliser cet objectif, le niveau de sévérité à atteindre est de :

Pour réduire le niveau global du risque, il est possible de réduire le niveau de sévérité en prenant des mesures limitant les conséquences et l'ampleur du préjudice. Si le niveau de sévérité originel est important ou modéré, il est possible de le faire diminuer pour baisser le niveau global du risque. Si la sévérité est déjà faible, il n'est pas possible de la réduire et il convient alors de réduire la probabilité du préjudice. Il est possible d'œuvrer tout à la fois à la réduction de la sévérité et de la probabilité du préjudice.

8) Pour réaliser cet objectif, le niveau de probabilité à atteindre est de :

Pour réduire le niveau global du risque, il est possible de réduire le niveau de probabilité. Si le niveau de probabilité originel est important ou modéré, il est possible de le

faire diminuer pour baisser le niveau global du risque. Si la probabilité est déjà faible, il n'est pas possible de la réduire et il convient alors de réduire la sévérité du préjudice. Il est possible d'œuvrer tout à la fois à la réduction de la probabilité et de la sévérité du préjudice.

9) Existe-t-il des normes techniques applicables au SIA contenant des recommandations relatives aux conséquences du ou des préjudices ?

Les normes techniques peuvent contenir des recommandations permettant de limiter les conséquences du préjudice. Il convient de référencer et de prendre en compte ces recommandations. Il convient d'appliquer prioritairement les normes harmonisées ou les spécifications communes.

10) Ces recommandations ont-elles été appliquées ?

Il est impératif d'appliquer des normes techniques, lorsqu'elles existent, pour la conception et le développement de SIA respectueux des VUE. L'application des normes techniques est une bonne mesure de gestion des risques.

11) Paraît-il possible de réduire le niveau des conséquences du ou des préjudices sans porter atteinte à la performance du SIA et à la réalisation de la finalité poursuivie en adoptant d'autres mesures que celles prévues par des normes techniques ?

S'il n'existe pas de recommandations applicables, car il n'y a pas de norme technique applicable ou, s'il y en une, celle-ci est lacunaire, ou si l'application des recommandations des normes est insuffisante pour réduire le niveau des conséquences du préjudice alors il faut mettre en œuvre d'autres mesures. Il est important de prendre en compte la destination ou la finalité de l'utilisation du SIA mais aussi les caractéristiques de l'utilisateur et le contexte du SIA pour déterminer les mesures adéquates.

12) Existe-t-il des normes techniques applicables au SIA contenant des recommandations relatives à l'ampleur du ou des préjudices ?

Les normes techniques peuvent contenir des recommandations permettant de limiter l'ampleur du préjudice. Il convient de référencer et de prendre en compte ces recommandations. Il convient d'appliquer prioritairement les normes harmonisées ou les spécifications communes.

13) Ces recommandations ont-elles été appliquées ?

Il est impératif d'appliquer des normes techniques, lorsqu'elles existent, pour la conception et le développement de SIA respectueux des VUE. L'application des normes techniques est une bonne mesure de gestion des risques.

14) Paraît-il possible de réduire le niveau de l'ampleur du ou des préjudices sans porter atteinte à la performance du SIA et à la réalisation de la finalité poursuivie en adoptant d'autres mesures que celles prévues par des normes techniques ?

S'il n'existe pas de recommandations applicables, car il n'y a pas de norme technique applicable ou, s'il y en une, celle-ci est lacunaire, ou si l'application des recommandations des normes est insuffisante pour réduire le niveau d'ampleur du préjudice alors il faut mettre en œuvre d'autres mesures. Il est important de prendre en compte la destination ou la finalité de l'utilisation du SIA mais aussi les caractéristiques de l'utilisateur et le contexte du SIA pour déterminer les mesures adéquates.

15) Existe-t-il des normes techniques applicables au SIA contenant des recommandations relatives à la probabilité de survenance du ou des préjudices ?

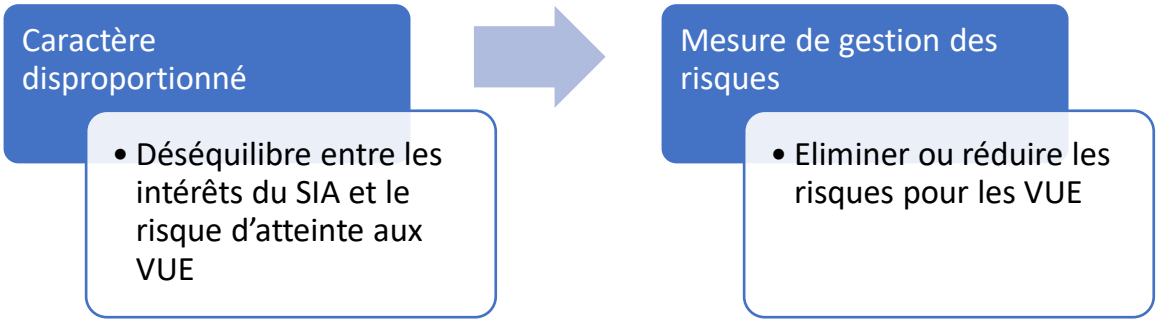
Les normes techniques peuvent contenir des recommandations permettant de limiter la probabilité de survenance du préjudice. Il convient de référencer et de prendre en compte ces recommandations. Il convient d'appliquer prioritairement les normes harmonisées ou les spécifications communes.

16) Ces recommandations ont-elles été appliquées ?

Il est impératif d'appliquer des normes techniques, lorsqu'elles existent, pour la conception et le développement de SIA respectueux des VUE. L'application des normes techniques est une bonne mesure de gestion des risques.

17) Paraît-il possible de réduire le niveau de probabilité du ou des préjudices sans porter atteinte à la performance du SIA et à la réalisation de la finalité poursuivie en adoptant d'autres mesures que celles prévues par des normes techniques ?

S'il n'existe pas de recommandations applicables, car il n'y a pas de norme technique applicable ou, s'il y en une, celle-ci est lacunaire, ou si l'application des recommandations des normes est insuffisante pour réduire le niveau de probabilité de survenance du préjudice alors il faut mettre en œuvre d'autres mesures. Il est important de prendre en compte la destination ou la finalité de l'utilisation du SIA mais aussi les caractéristiques de l'utilisateur et le contexte du SIA pour déterminer les mesures adéquates.

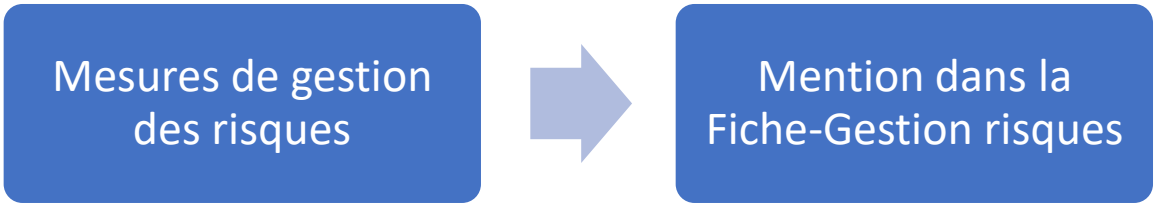


126. La prise en compte de l'utilisateur et du contexte du SIA. Selon l'AI Act, les mesures de gestion des risques doivent prendre en compte les connaissances techniques, l'expérience, l'éducation, la formation pouvant être attendues de l'utilisateur et le contexte dans lequel le système est destiné à être utilisé (AI Act, art. 9, §5).

Cela signifie que si des mesures de gestion des risques génériques peuvent être identifiées, telles qu'elles résultent de normes techniques par exemple, celles-ci ne sauraient être nécessairement appliquée telles quelles sans prise en compte du contexte de déploiement du SIA, c'est-à-dire les caractéristiques des utilisateurs et les conditions matérielles, géographiques et temporelles. Les mesures de gestion de risques doivent être compatibles avec le profil de l'utilisateur et le contexte de déploiement du SIA. Cette compatibilité est un élément essentiel de l'efficacité des mesures de gestion des risques.

L'adoption de mesures de gestion des risques compatibles avec le profil de l'utilisateur et le contexte suppose d'avoir une bonne connaissance des caractéristiques des utilisateurs et de ce contexte. Un dialogue entre l'ensemble des parties impliquées dans le développement et le déploiement du SIA est dans ce cadre fondamental.

127. La mention des mesures de gestion des risques adoptées dans la Fiche-gestion risques VUE. Les mesures de gestion des risques adoptées doivent être mentionnées dans la Fiche-Gestion risques VUE. Il convient de les décrire précisément et d'indiquer les problèmes qu'elles résolvent.



c. L'évaluation des effets des mesures de gestion des risques

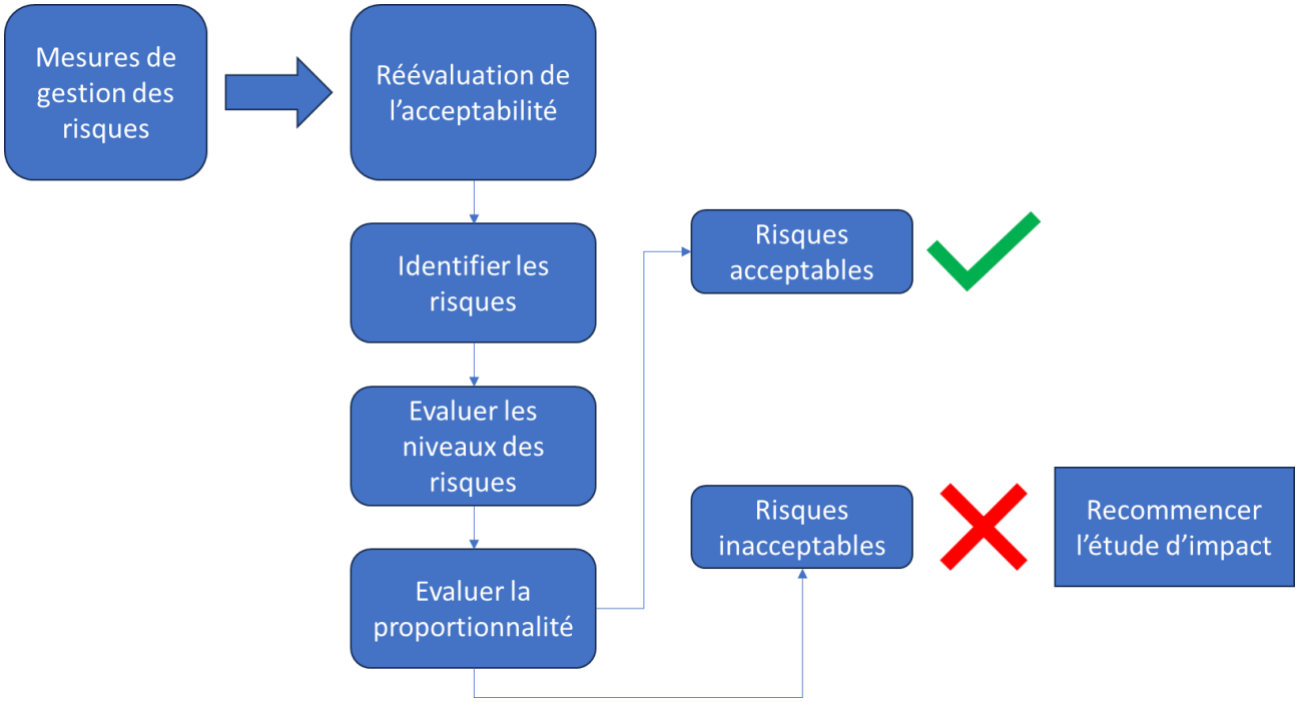
128. La conclusion de l'étude d'impact : la réévaluation de l'acceptabilité des risques. Enfin, il faut évaluer l'effet des mesures de gestion de risques sur l'acceptabilité des risques. A cette fin, une réévaluation du niveau des risques et de leur proportionnalité est nécessaire.

La réévaluation du niveau de risque et de la proportionnalité du risque consiste à réaliser une seconde fois l'étape 2 consistant à identifier les risques et à évaluer les niveaux des risques puis la proportionnalité du SIA sur la base des nouveaux paramètres découlant de l'application des mesures de gestion des risques.

Deux cas de figure peuvent se présenter :

- soit les risques sont proportionnés et donc acceptables : dans ce cas, l'étude d'impact donne un résultat positif et doit être considérée comme achevée ;
- soit un ou plusieurs risques demeurent disproportionnés et donc inacceptables : dans ce cas, il convient de reprendre l'étude d'impact depuis le début en repensant la conception du SIA au regard des résultats déjà fournis par l'étude d'impact précédente.

Ces résultats doivent être reportés dans le *Tableau synthétique de l'étude d'impact.*



4. Conclusion : Tableau synthétique de l'étude d'impact sur les VUE (annexe 7)

129. Le contenu du Tableau synthétique de l'étude d'impact sur les VUE. Les principaux éléments et les résultats de l'étude d'impact doivent être reportés dans le *Tableau synthétique de l'étude d'impact*. Ce tableau comprend :

- Les risques identifiées et les VUE concernées ;
- Le niveau des risques et leur proportionnalité ;
- Les mesures de gestion des risques adoptées permettant de proportionner le risque.

130. Faire figurer les résultats de l'étude d'impact sur les VUE dans la documentation relative au SIA. Le *Tableau synthétique de l'étude d'impact* à vocation à figurer dans la documentation relative au SIA aux fins d'information des déployeurs et utilisateurs finaux du SIA.

Ce tableau synthétique peut être intégré à la documentation technique régie par l'article 11 et l'annexe IV de l'AI Act.

---

[149] JANSSEN Heleen *et al.*, « Practical fundamental rights impact assessments », *International Journal of Law and Information Technology,* vol. 30, issue 2, 2022, p. 200-232.
[150] Un SIA est considéré comme étant à haut risque compte tenu de sa fonction, de sa finalité et des modalités spécifiques. C'est parce qu'il a certaines fonctions, finalités et modalités spécifiques qu'il présente un haut risque. V. AI Act, 21 avr. 2021, 2021/0106 (COD), Exposé des motifs, p. 15.
[151] Par ex., l'article 9, §5 de l'AI Act énonce que les mesures de gestion des risques « sont telles que tout risque résiduel associé à chaque danger ainsi que le risque résiduel global lié aux systèmes d'IA à haut risque sont jugés acceptables ».
[152] V. JANSSEN Heleen *et al.*, « Practical fundamental rights impact assessments », *International Journal of Law and Information Technology,* vol. 30, issue 2, 2022, p. 216.

[153] RGPD, cons. 75 et 90 et art. 24, 1 ; v. égal. G29, *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*, 4 oct. 2017, WP 248 rév. 01 et Cnil, *PIA : Les bases de connaissance*, févr. 2018.
[154] C. civ., art. 1246 à 1252.
[155] Les notions de préjudice et de dommage peuvent être distinguées en droit. L'AI Act retenant une conception unifiée en n'évoquant que le préjudice, le terme de préjudice sera ici favorisé.
[156] Cnil, *PIA : Les bases de connaissance*, févr. 2018, p. 3.
[157] V. en ce sens, ALIGNER, *How to use the ALIGNER Fundamental Rights Impact Assessment template*, WP4. Disponible sur : https://aligner-h2020.eu/fundamental-rights-impact-assessment-fria/ (consulté le 16 jan. 2024).
[158] Ce critère est celui principalement retenu par la Cnil dans le cadre de l'analyse d'impact relative à la protection des données. V. Cnil, *PIA : Les bases de connaissance*, févr. 2018, p. 3-4. Le DSA s'attache également à ce critère de l'irréversibilité ou la difficulté de remédier au problème pour définir le risque systémique (cons. 79).
[159] Règl. 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), *JOUE*, L 277, 27 oct. 2022, p. 1–102
[160] L'AI Act distingue les notions de SIA et de modèle d'IA. Il est indiqué dans le cons. 97 : « Bien que les modèles d'IA soient des composants essentiels des systèmes d'IA, ils ne constituent pas en soi des systèmes d'IA. Les modèles d'IA nécessitent l'ajout d'autres composants, tels qu'une interface utilisateur, pour devenir des systèmes d'IA. »
[161] G29, *Lignes directrices concernant les délégués à la protection des données (DPD)*, 5 avr. 2017, WP 243 rev.01, p. 9
[162] Dir. (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), *JOUE*, L 333, 27.12.2022, p. 80–152.
[163] Cnil, *PIA : Les bases de connaissance*, févr. 2018, p. 5.
[164] Cnil, *PIA : Les bases de connaissance*, févr. 2018, p. 5.
[165] NIST, *AI Risk Management Framework: Initial Draft*, p.9.
[166] ISO/IEC TS 5723:2022 – Trustworthiness — Vocabulary : « 3.2.2 accuracy : measure of closeness of results of observations, computations, or estimates to the true values or the values accepted as being true »
[167] ISO/IEC TS 5723:2022 – Trustworthiness — Vocabulary : « 3.2.16 robustness : ability of a system (3.3.10) to maintain its level of performance under a variety of circumstances »
[168] ISO/IEC TS 5723:2022 – Trustworthiness — Vocabulary : « 3.2.15 resilience system : capability (3.3.2) of a system (3.3.10) to maintain its functions and structure in the face of internal and external change, and to degrade gracefully when this is necessary »
[169] ISO/IEC TS 5723:2022 – Trustworthiness — Vocabulary : « 3.2.18 security : resistance to intentional, unauthorized act(s) designed to cause harm or damage to a system (3.3.10) »
[170] Pour une étude détaillée, v. MAXWELL J. Winston, « Le contrôle humain pour détecter les erreurs algorithmiques » *In* CASTETS-RENARD Céline et EYNARD Jessica (dir.), *op. cit.*, p. 707-748.
[171] Les normes harmonisées sont des normes techniques dont les références ont été publiées au Journal officiel de l'Union européenne.
[172] Les spécifications communes sont des normes adoptées par la Commission européenne en cas d'absence de norme technique satisfaisante.
[173] Des organisations retiennent trois niveaux de risques comme la Commission nationale consultative des droits de l'Homme (CNCDH, *Avis A-2022-6 relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux*, 7 avril 2022, p. 19). V. égal. JANSSEN Heleen *et al*., « Practical fundamental rights impact assessments », *International Journal of Law and Information Technology,* vol. 30, issue 2, 2022, p. 218 : « From the risks identified by considering the relevant factors and the likeliness of occurrence of these risks, an aggregated risk 'score' should be developed. This score should result, for instance, in a determination of 'high', 'medium' or 'low' risk for each right to be infringed by the system (other rankings are of course possible and may be more appropriate in different circumstances) ».
[174] Par ex., l'article 9, §5 de l'AI Act énonce que les mesures de gestion des risques « sont telles que tout risque résiduel associé à chaque danger ainsi que le risque résiduel global lié aux systèmes d'IA à haut risque sont jugés acceptables ».
[175] XYNOPOULOS George, « Proportionnalité », In ALLAND Denis et RIALS Stéphane (dir.), *Dictionnaire de la culture juridique*, Paris : PUF, 2003, p. 1251. V. égal. DUCOULOMBIER Peggy, *Les conflits de droits fondamentaux devant la Cour européenne des droits de l'homme*, Bruxelles : Bruylant, 2011, spéc. p. 370 et s. ; GAUTHIER Catherine, « Le contrôle de proportionnalité dans la jurisprudence de la Cour européenne des droits

de l'homme », *AJDA*, 2021, p. 793 ; SAUVE Jean-Marc, « Le principe de proportionnalité, protecteur des libertés ? », *Les cahiers de Portalis*, 2018, n° 5, p. 11.

[176] TINIERE Romain et VIAL Claire, *Droit de l'Union européenne des droits fondamentaux*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 2023, p. 314.

[177] Van Drooghenbroeck, S. et Rizcallah, C., « Article 52-1. - Limitations aux droits garantis » in Picod, F. et al. (dir.), Charte des droits fondamentaux de l'Union européenne, 3e édition, Bruxelles, Bruylant, 2023, p. 1377.

[178] TINIERE Romain et VIAL Claire, *Droit de l'Union européenne des droits fondamentaux*, Bruxelles : Bruylant, coll. Droit de l'Union européenne, 2023, p. 314-315.

[179] Par opposition au contrôle de proportionnalité *lato sensu* qui désigne le contrôle de proportionnalité dans sa globalité c'est-à-dire l'appréciation du caractère approprié, nécessaire et proportionné d'une atteinte.

[180] JANSSEN Heleen *et al*., « Practical fundamental rights impact assessments », *International Journal of Law and Information Technology,* vol. 30, issue 2, 2022, p. 200-232

[181] V. *supra*, n° 113.

[182] Sur l'intervention des autorités de surveillance en cas de risque d'un SIA, v. AI Act, art. 79, §2.

[183] Par exemple, le RGPD évoque dans son article 26 relatif à la protection des données dès la conception et par défaut la nécessité pour le responsable du traitement de prendre des mesures techniques et organisationnelles appropriées afin de protéger les droits des personnes.

Annexes

Table des annexes :

Annexe 1 : Définitions

Terme	Définition	Source
AI Act	Règlement de l'Union européenne sur l'intelligence artificielle	Règlement (UE) 2024/1689 du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle).
Ampleur du préjudice	Diffusion du préjudice au sein de la société.	
Chaîne de valeur	Ensemble des activités de la conception à l'exploitation du SIA impliquant divers opérateurs, tels les fournisseurs, les déployeurs, les fabricants de produits, les mandataires, les distributeurs et les importateurs.	
Conséquences du préjudice	Effets du préjudice sur une personne physique ou morale.	
Cour de justice de l'Union européenne (CJUE)	Juridiction de l'Union européenne appliquant le droit de l'Union.	
Cour européenne des droits de l'Homme (CEDH)	Juridiction internationale contrôle le respect de la Convention européenne des droits de l'Homme par les États signataires (46 pays).	
Cybersécurité	Resistance to intentional, unauthorized act(s) designed to cause harm or damage to a system.	ISO/IEC TS 5723:2022 – Trustworthiness — Vocabulary

Cycle de vie	Evolution of an AI system from inception through retirement.	ISO/IEC 22989: 2022 – Information technology — Artificial intelligence — Artificial intelligence concepts and terminology
Déployeur	Personne physique ou morale, une autorité publique, une agence ou un autre organisme utilisant sous sa propre autorité un système d'IA sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel.	AI Act, art. 3, §4
Destination	Utilisation à laquelle un système d'IA est destiné par le fournisseur, y compris le contexte et les conditions spécifiques d'utilisation, tels qu'ils sont précisés dans les informations communiquées par le fournisseur dans la notice d'utilisation, les indications publicitaires ou de vente et les déclarations, ainsi que dans la documentation technique	AI Act, art. 3, §12
Donnée à caractère non personnel	Données autres que les données à caractère personnel.	AI Act, art. 3, §51
Donnée à caractère personnel	Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.	RGPD, art. 4, §1

Données biométriques	Données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, telles que des images faciales ou des données dactyloscopiques.	AI Act, art. 3, §34
Données d'entraînement	Données utilisées pour entraîner un système d'IA en ajustant ses paramètres entraînables.	AI Act, art. 3, §29
Données d'entrée	Données fournies à un système d'IA ou directement acquises par celui-ci et à partir desquelles il produit une sortie;	AI Act, art. 3, §33
Données de test	Données utilisées pour fournir une évaluation indépendante du système d'IA afin de confirmer la performance attendue de ce système avant sa mise sur le marché ou sa mise en service.	AI Act, art. 3, §32
Données de validation	Données utilisées pour fournir une évaluation du système d'IA entraîné et pour régler ses paramètres non entraînables ainsi que son processus d'apprentissage, afin, notamment, d'éviter tout sous-ajustement ou surajustement.	AI Act, art. 3, §30
Données sensibles ou catégories particulières de données à caractère personnel	Traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.	RGPD, art. 9, §1

Exactitude	Measure of closeness of results of observations, computations, or estimates to the true values or the values accepted as being true.	ISO/IEC TS 5723:2022 – Trustworthiness — Vocabulary
Finalité	Objectif poursuivi par le déployeur du SIA.	
Fonctions	Tâches et opérations pouvant être réalisées par le SIA.	
Fournisseur	Personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA ou un modèle d'IA à usage général et le met sur le marché ou met le système d'IA en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit.	AI Act, art. 3, §3
Hypertrucage	Image ou contenu audio ou vidéo généré ou manipulé par l'IA, présentant une ressemblance avec des personnes, des objets, des lieux, des entités ou événements existants et pouvant être perçu à tort par une personne comme authentiques ou véridiques.	AI Act, art. 3, §60
Identification biométrique	Reconnaissance automatisée de caractéristiques physiques, physiologiques, comportementales ou psychologiques humaines aux fins d'établir l'identité d'une personne physique en comparant ses données biométriques à des données biométriques de personnes stockées dans une base de données.	AI Act, art. 3, §35
Incident grave	Incident ou dysfonctionnement d'un système d'IA entraînant directement ou indirectement : a) le décès d'une personne ou une atteinte grave à la santé d'une personne ; b) une perturbation grave et irréversible de la gestion ou du fonctionnement d'infrastructures critiques ; c) la violation des obligations au titre du droit de l'Union visant	AI Act, art. 3, §49

	à protéger les droits fondamentaux ; d) un dommage grave à des biens ou à l'environnement.	
Infraction de grande ampleur	Tout acte ou toute omission contraire au droit de l'Union en matière de protection des intérêts des personnes, qui : a) a porté ou est susceptible de porter atteinte aux intérêts collectifs des personnes résidant dans au moins deux États membres autres que celui : i) où l'acte ou l'omission en question a son origine ou a eu lieu ; ii) où le fournisseur concerné ou, le cas échéant, son mandataire, est situé ou établi; ou iii) où le déployeur est établi, lorsque l'infraction est commise par le déployeur ; b) a porté, porte ou est susceptible de porter atteinte aux intérêts collectifs des personnes, qui présente des caractéristiques communes, notamment la même pratique illégale ou la violation du même intérêt, et qui se produit simultanément, commise par le même opérateur, dans au moins trois États membres.	AI Act, art. 3, §61
Infrastructure critique	Bien, installation, équipement, réseau ou système, ou partie d'un bien, d'une installation, d'un équipement, d'un réseau ou d'un système, qui est nécessaire à la fourniture d'un service essentiel.	Dir. 2022/2557, art. 2, §4
Jeu de données de validation	Jeu de données distinct ou une partie du jeu de données d'entraînement, sous la forme d'une division variable ou fixe.	AI Act, art. 3, §31
Maîtrise de l'IA	Compétences, connaissances et compréhension qui permettent aux fournisseurs, aux déployeurs et aux personnes concernées, compte tenu de leurs droits et obligations respectifs dans le contexte de l'AI Act, de	AI Act, art. 3, §56

	procéder à un déploiement des systèmes d'IA en toute connaissance de cause, ainsi que de prendre conscience des possibilités et des risques que comporte l'IA, ainsi que des préjudices potentiels qu'elle peut causer;	
Mauvaise utilisation raisonnablement prévisible	Utilisation d'un système d'IA d'une manière qui n'est pas conforme à sa destination, mais qui peut résulter d'un comportement humain raisonnablement prévisible ou d'une interaction raisonnablement prévisible avec d'autres systèmes, y compris d'autres systèmes d'IA.	AI Act, art. 3, §13
Modèle d'IA à usage général	Modèle d'IA, y compris lorsque ce modèle d'IA est entraîné à l'aide d'un grand nombre de données utilisant l'auto-supervision à grande échelle, qui présente une généralité significative et est capable d'exécuter de manière compétente un large éventail de tâches distinctes, indépendamment de la manière dont le modèle est mis sur le marché, et qui peut être intégré dans une variété de systèmes ou d'applications en aval, à l'exception des modèles d'IA utilisés pour des activités de recherche, de développement ou de prototypage avant leur mise sur le marché.	AI Act, art. 3, §63
Modification substantielle	Modification apportée à un système d'IA après sa mise sur le marché ou sa mise en service, qui n'est pas prévue ou planifiée dans l'évaluation initiale de la conformité réalisée par le fournisseur et qui a pour effet de nuire à la conformité de ce système aux exigences énoncées au chapitre III, section 2, ou qui entraîne une modification de la destination pour laquelle le système d'IA a été évalué.	AI Act, art. 3, §23

Norme harmonisée	Norme européenne adoptée sur la base d'une demande formulée par la Commission pour l'application de la législation d'harmonisation de l'Union.	AI Act, art. 3, §27
Performance d'un système d'IA	Capacité d'un système d'IA à remplir sa destination.	AI Act, art. 3, §18
Préjudice	Dommage subi par une personne.	
Probabilité de survenance du préjudice	Eventualité que le préjudice se déclare.	
Profilage	Toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.	RGPD, art. 4, §4
Résilience	Capability of a system to maintain its functions and structure in the face of internal and external change, and to degrade gracefully when this is necessary	ISO/IEC TS 5723:2022 – Trustworthiness — Vocabulary
RGPD	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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).	

Risque	Combinaison de la probabilité d'un préjudice et de la sévérité de celui-ci.	AI Act, art. 3, §2
Risque systémique	Risque spécifique aux capacités à fort impact des modèles d'IA à usage général, ayant une incidence significative sur le marché de l'Union en raison de leur portée ou d'effets négatifs réels ou raisonnablement prévisibles sur la santé publique, la sûreté, la sécurité publique, les droits fondamentaux ou la société dans son ensemble, pouvant être propagé à grande échelle tout au long de la chaîne de valeur.	AI Act, art. 3, §65
Robustesse	Ability of a system to maintain its level of performance under a variety of circumstances.	ISO/IEC TS 5723:2022 – Trustworthiness — Vocabulary
Spécification commune	Ensemble de spécifications techniques qui permettent de satisfaire à certaines exigences établies en vertu de l'AI Act.	AI Act, art. 3, §28
Système d'IA	Système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels.	AI Act, art. 3, §1
Système de catégorisation biométrique	Système d'IA destiné à affecter des personnes physiques à des catégories spécifiques sur la base de leurs données biométriques, à moins que cela ne soit accessoire à un autre service commercial et strictement nécessaire pour des raisons techniques objectives.	AI Act, art. 3, §40

Système de reconnaissance des émotions	Système d'IA permettant la reconnaissance ou la déduction des émotions ou des intentions de personnes physiques sur la base de leurs données biométriques.	AI Act, art. 3, §39
Système de surveillance après commercialisation	Ensemble des activités réalisées par les fournisseurs de systèmes d'IA pour recueillir et analyser les données issues de l'expérience d'utilisation des systèmes d'IA qu'ils mettent sur le marché ou mettent en service de manière à repérer toute nécessité d'appliquer immédiatement une mesure préventive ou corrective.	AI Act, art. 3, §25
Système d'IA à usage général	Système d'IA qui est fondé sur un modèle d'IA à usage général et qui a la capacité de répondre à diverses finalités, tant pour une utilisation directe que pour une intégration dans d'autres systèmes d'IA.	AI Act, art. 3, §66
Système d'identification biométrique à distance	Système d'IA destiné à identifier des personnes physiques sans leur participation active, généralement à distance, en comparant les données biométriques d'une personne avec celles qui figurent dans une base de données.	AI Act, art. 3, §41
Système d'identification biométrique à distance *a posteriori*	Système d'identification biométrique à distance autre qu'un système d'identification biométrique à distance en temps réel.	AI Act, art. 3, §43
Système d'identification biométrique à distance en temps réel	Système d'identification biométrique à distance dans lequel l'acquisition des données biométriques, la comparaison et l'identification se déroulent sans décalage temporel important et qui comprend non seulement l'identification instantanée, mais aussi avec un léger décalage afin d'éviter tout contournement des règles.	AI Act, art. 3, §42

Valeurs de l'Union européenne (VUE)	Valeurs fondamentales de l'Union européenne énoncées par l'article 2 du Traité sur l'Union européenne (TUE). Il s'agit de la dignité humaine, de la liberté, de la démocratie, de l'égalité, de l'État de droit, ainsi que du respect des droits de l'Homme.	
Vérification biométrique	Vérification « un à un » automatisée, y compris l'authentification, de l'identité des personnes physiques en comparant leurs données biométriques à des données biométriques précédemment fournies.	AI Act, art. 3, §36

Annexe 2 : Charte des droits fondamentaux de l'Union européenne

Le Parlement européen, le Conseil et la Commission proclament solennellement en tant que Charte des droits fondamentaux de l'Union européenne le texte repris ci-après.

CHARTE DES DROITS FONDAMENTAUX DE L'UNION EUROPÉENNE

Les peuples d'Europe, en établissant entre eux une union sans cesse plus étroite, ont décidé de partager un avenir pacifique fondé sur des valeurs communes.

Consciente de son patrimoine spirituel et moral, l'Union se fonde sur les valeurs indivisibles et universelles de dignité humaine, de liberté, d'égalité et de solidarité; elle repose sur le principe de la démocratie et le principe de l'État de droit. Elle place la personne au cœur de son action en instituant la citoyenneté de l'Union et en créant un espace de liberté, de sécurité et de justice.

L'Union contribue à la préservation et au développement de ces valeurs communes dans le respect de la diversité des cultures et des traditions des peuples d'Europe, ainsi que de l'identité nationale des États membres et de l'organisation de leurs pouvoirs publics aux niveaux national, régional et local; elle cherche à promouvoir un développement équilibré et durable et assure la libre circulation des personnes, des services, des marchandises et des capitaux, ainsi que la liberté d'établissement.

À cette fin, il est nécessaire, en les rendant plus visibles dans une Charte, de renforcer la protection des droits fondamentaux à la lumière de l'évolution de la société, du progrès social et des développements scientifiques et technologiques.

La présente Charte réaffirme, dans le respect des compétences et des tâches de l'Union, ainsi que du principe de subsidiarité, les droits qui résultent notamment des traditions constitutionnelles et des obligations internationales communes aux États membres, de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, des Chartes sociales adoptées par l'Union et par le Conseil de l'Europe, ainsi que de la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'Homme. Dans ce contexte, la Charte sera interprétée par les juridictions de l'Union et des États membres en prenant dûment en considération les explications établies sous l'autorité du praesidium de la Convention qui a élaboré la Charte et mises à jour sous la responsabilité du praesidium de la Convention européenne.

La jouissance de ces droits entraîne des responsabilités et des devoirs tant à l'égard d'autrui qu'à l'égard de la communauté humaine et des générations futures.

En conséquence, l'Union reconnaît les droits, les libertés et les principes énoncés ci-après.

TITRE I : DIGNITÉ

Article 1

Dignité humaine

La dignité humaine est inviolable. Elle doit être respectée et protégée.

Article 2

Droit à la vie

1. Toute personne a droit à la vie.
2. Nul ne peut être condamné à la peine de mort, ni exécuté.

Article 3

Droit à l'intégrité de la personne

1. Toute personne a droit à son intégrité physique et mentale.
2. Dans le cadre de la médecine et de la biologie, doivent notamment être respectés:

a)le consentement libre et éclairé de la personne concernée, selon les modalités définies par la loi;

b)l'interdiction des pratiques eugéniques, notamment celles qui ont pour but la sélection des personnes;

c)l'interdiction de faire du corps humain et de ses parties, en tant que tels, une source de profit;

d) l'interdiction du clonage reproductif des êtres humains.

Article 4

Interdiction de la torture et des peines ou traitements inhumains ou dégradants

Nul ne peut être soumis à la torture, ni à des peines ou traitements inhumains ou dégradants.

Article 5

Interdiction de l'esclavage et du travail forcé

1. Nul ne peut être tenu en esclavage ni en servitude.
2. Nul ne peut être astreint à accomplir un travail forcé ou obligatoire.
3. La traite des êtres humains est interdite.

TITRE II : LIBERTÉS

Article 6

Droit à la liberté et à la sûreté

Toute personne a droit à la liberté et à la sûreté.

Article 7

Respect de la vie privée et familiale

Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.

Article 8

Protection des données à caractère personnel

1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

Article 9

Droit de se marier et droit de fonder une famille

Le droit de se marier et le droit de fonder une famille sont garantis selon les lois nationales qui en régissent l'exercice.

Article 10

Liberté de pensée, de conscience et de religion

1. Toute personne a droit à la liberté de pensée, de conscience et de religion. Ce droit implique la liberté de changer de religion ou de conviction, ainsi que la liberté de manifester sa religion ou sa conviction individuellement ou collectivement, en public ou en privé, par le culte, l'enseignement, les pratiques et l'accomplissement des rites.

2. Le droit à l'objection de conscience est reconnu selon les lois nationales qui en régissent l'exercice.

Article 11

Liberté d'expression et d'information

1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières.

2. La liberté des médias et leur pluralisme sont respectés.

Article 12

Liberté de réunion et d'association

1. Toute personne a droit à la liberté de réunion pacifique et à la liberté d'association à tous les niveaux, notamment dans les domaines politique, syndical et civique, ce qui implique le droit de toute personne de fonder avec d'autres des syndicats et de s'y affilier pour la défense de ses intérêts.

2. Les partis politiques au niveau de l'Union contribuent à l'expression de la volonté politique des citoyens de l'Union.

Article 13

Liberté des arts et des sciences

Les arts et la recherche scientifique sont libres. La liberté académique est respectée.

Article 14

Droit à l'éducation

1. Toute personne a droit à l'éducation, ainsi qu'à l'accès à la formation professionnelle et continue.

2. Ce droit comporte la faculté de suivre gratuitement l'enseignement obligatoire.

3. La liberté de créer des établissements d'enseignement dans le respect des principes démocratiques, ainsi que le droit des parents d'assurer l'éducation et l'enseignement de leurs enfants conformément à leurs convictions religieuses, philosophiques et pédagogiques, sont respectés selon les lois nationales qui en régissent l'exercice.

Article 15

Liberté professionnelle et droit de travailler

1. Toute personne a le droit de travailler et d'exercer une profession librement choisie ou acceptée.

2. Tout citoyen de l'Union a la liberté de chercher un emploi, de travailler, de s'établir ou de fournir des services dans tout État membre.

3. Les ressortissants des pays tiers qui sont autorisés à travailler sur le territoire des États membres ont droit à des conditions de travail équivalentes à celles dont bénéficient les citoyens de l'Union.

Article 16

Liberté d’entreprise

La liberté d’entreprise est reconnue conformément au droit de l’Union et aux législations et pratiques nationales.

Article 17

Droit de propriété

1. Toute personne a le droit de jouir de la propriété des biens qu’elle a acquis légalement, de les utiliser, d’en disposer et de les léguer. Nul ne peut être privé de sa propriété, si ce n’est pour cause d’utilité publique, dans des cas et conditions prévus par une loi et moyennant en temps utile une juste indemnité pour sa perte. L’usage des biens peut être réglementé par la loi dans la mesure nécessaire à l’intérêt général.

2. La propriété intellectuelle est protégée.

Article 18

Droit d’asile

Le droit d’asile est garanti dans le respect des règles de la convention de Genève du 28 juillet 1951 et du protocole du 31 janvier 1967 relatifs au statut des réfugiés et conformément au traité sur l’Union européenne et au traité sur le fonctionnement de l’Union européenne (ci-après dénommés "les traités").

Article 19

Protection en cas d’éloignement, d’expulsion et d’extradition

1. Les expulsions collectives sont interdites.

2. Nul ne peut être éloigné, expulsé ou extradé vers un État où il existe un risque sérieux qu’il soit soumis à la peine de mort, à la torture ou à d’autres peines ou traitements inhumains ou dégradants.

TITRE III : ÉGALITÉ

Article 20

Égalité en droit

Toutes les personnes sont égales en droit.

Article 21

Non-discrimination

1. Est interdite toute discrimination fondée notamment sur le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge ou l'orientation sexuelle.

2. Dans le domaine d'application des traités et sans préjudice de leurs dispositions particulières, toute discrimination exercée en raison de la nationalité est interdite.

Article 22

Diversité culturelle, religieuse et linguistique

L'Union respecte la diversité culturelle, religieuse et linguistique.

Article 23

Égalité entre femmes et hommes

L'égalité entre les femmes et les hommes doit être assurée dans tous les domaines, y compris en matière d'emploi, de travail et de rémunération.

Le principe de l'égalité n'empêche pas le maintien ou l'adoption de mesures prévoyant des avantages spécifiques en faveur du sexe sous-représenté.

Article 24

Droits de l'enfant

1. Les enfants ont droit à la protection et aux soins nécessaires à leur bien-être. Ils peuvent exprimer leur opinion librement. Celle-ci est prise en considération pour les sujets qui les concernent, en fonction de leur âge et de leur maturité.

2. Dans tous les actes relatifs aux enfants, qu'ils soient accomplis par des autorités publiques ou des institutions privées, l'intérêt supérieur de l'enfant doit être une considération primordiale.

3. Tout enfant a le droit d'entretenir régulièrement des relations personnelles et des contacts directs avec ses deux parents, sauf si cela est contraire à son intérêt.

Article 25

Droits des personnes âgées

L'Union reconnaît et respecte le droit des personnes âgées à mener une vie digne et indépendante et à participer à la vie sociale et culturelle.

Article 26

Intégration des personnes handicapées

L'Union reconnaît et respecte le droit des personnes handicapées à bénéficier de mesures visant à assurer leur autonomie, leur intégration sociale et professionnelle et leur participation à la vie de la communauté.

TITRE IV : SOLIDARITÉ

Article 27

Droit à l'information et à la consultation des travailleurs au sein de l'entreprise

Les travailleurs ou leurs représentants doivent se voir garantir, aux niveaux appropriés, une information et une consultation en temps utile, dans les cas et conditions prévus par le droit de l'Union et les législations et pratiques nationales.

Article 28

Droit de négociation et d'actions collectives

Les travailleurs et les employeurs, ou leurs organisations respectives, ont, conformément au droit de l'Union et aux législations et pratiques nationales, le droit de négocier et de conclure des conventions collectives aux niveaux appropriés et de recourir, en cas de conflits d'intérêts, à des actions collectives pour la défense de leurs intérêts, y compris la grève.

Article 29

Droit d'accès aux services de placement

Toute personne a le droit d'accéder à un service gratuit de placement.

Article 30

Protection en cas de licenciement injustifié

Tout travailleur a droit à une protection contre tout licenciement injustifié, conformément au droit de l'Union et aux législations et pratiques nationales.

Article 31

Conditions de travail justes et équitables

1. Tout travailleur a droit à des conditions de travail qui respectent sa santé, sa sécurité et sa dignité.

2. Tout travailleur a droit à une limitation de la durée maximale du travail et à des périodes de repos journalier et hebdomadaire, ainsi qu'à une période annuelle de congés payés.

Article 32

Interdiction du travail des enfants et protection des jeunes au travail

Le travail des enfants est interdit. L'âge minimal d'admission au travail ne peut être inférieur à l'âge auquel cesse la période de scolarité obligatoire, sans préjudice des règles plus favorables aux jeunes et sauf dérogations limitées.

Les jeunes admis au travail doivent bénéficier de conditions de travail adaptées à leur âge et être protégés contre l'exploitation économique ou contre tout travail susceptible de nuire à leur sécurité, à leur santé, à leur développement physique, mental, moral ou social ou de compromettre leur éducation.

Article 33

Vie familiale et vie professionnelle

1. La protection de la famille est assurée sur le plan juridique, économique et social.

2. Afin de pouvoir concilier vie familiale et vie professionnelle, toute personne a le droit d'être protégée contre tout licenciement pour un motif lié à la maternité, ainsi que le droit à un congé de maternité payé et à un congé parental à la suite de la naissance ou de l'adoption d'un enfant.

Article 34

Sécurité sociale et aide sociale

1. L'Union reconnaît et respecte le droit d'accès aux prestations de sécurité sociale et aux services sociaux assurant une protection dans des cas tels que la maternité, la maladie, les accidents du travail, la dépendance ou la vieillesse, ainsi qu'en cas de perte d'emploi, selon les règles établies par le droit de l'Union et les législations et pratiques nationales.

2. Toute personne qui réside et se déplace légalement à l'intérieur de l'Union a droit aux prestations de sécurité sociale et aux avantages sociaux, conformément au droit de l'Union et aux législations et pratiques nationales.

3. Afin de lutter contre l'exclusion sociale et la pauvreté, l'Union reconnaît et respecte le droit à une aide sociale et à une aide au logement destinées à assurer une existence digne à tous ceux qui ne disposent pas de ressources suffisantes, selon les règles établies par le droit de l'Union et les législations et pratiques nationales.

Article 35

Protection de la santé

Toute personne a le droit d'accéder à la prévention en matière de santé et de bénéficier de soins médicaux dans les conditions établies par les législations et pratiques nationales. Un niveau élevé de protection de la santé humaine est assuré dans la définition et la mise en œuvre de toutes les politiques et actions de l'Union.

Article 36

Accès aux services d'intérêt économique général

L’Union reconnaît et respecte l’accès aux services d’intérêt économique général tel qu’il est prévu par les législations et pratiques nationales, conformément aux traités, afin de promouvoir la cohésion sociale et territoriale de l’Union.

Article 37

Protection de l’environnement

Un niveau élevé de protection de l’environnement et l’amélioration de sa qualité doivent être intégrés dans les politiques de l’Union et assurés conformément au principe du développement durable.

Article 38

Protection des consommateurs

Un niveau élevé de protection des consommateurs est assuré dans les politiques de l’Union.

TITRE V : CITOYENNETÉ

Article 39

Droit de vote et d’éligibilité aux élections au Parlement européen

1. Tout citoyen de l’Union a le droit de vote et d’éligibilité aux élections au Parlement européen dans l’État membre où il réside, dans les mêmes conditions que les ressortissants de cet État.

2. Les membres du Parlement européen sont élus au suffrage universel direct, libre et secret.

Article 40

Droit de vote et d’éligibilité aux élections municipales

Tout citoyen de l’Union a le droit de vote et d’éligibilité aux élections municipales dans l’État membre où il réside, dans les mêmes conditions que les ressortissants de cet État.

Article 41

Droit à une bonne administration

1. Toute personne a le droit de voir ses affaires traitées impartialement, équitablement et dans un délai raisonnable par les institutions, organes et organismes de l’Union.

2. Ce droit comporte notamment:

a) le droit de toute personne d’être entendue avant qu’une mesure individuelle qui l’affecterait défavorablement ne soit prise à son encontre;

b) le droit d’accès de toute personne au dossier qui la concerne, dans le respect des intérêts légitimes de la confidentialité et du secret professionnel et des affaires;

c) l'obligation pour l'administration de motiver ses décisions.

3. Toute personne a droit à la réparation par l'Union des dommages causés par les institutions, ou par ses agents dans l'exercice de leurs fonctions, conformément aux principes généraux communs aux droits des États membres.

4. Toute personne peut s'adresser aux institutions de l'Union dans une des langues des traités et doit recevoir une réponse dans la même langue.

Article 42

Droit d'accès aux documents

Tout citoyen de l'Union ainsi que toute personne physique ou morale résidant ou ayant son siège statutaire dans un État membre a un droit d'accès aux documents des institutions, organes et organismes de l'Union, quel que soit leur support.

Article 43

Médiateur européen

Tout citoyen de l'Union ainsi que toute personne physique ou morale résidant ou ayant son siège statutaire dans un État membre a le droit de saisir le médiateur européen de cas de mauvaise administration dans l'action des institutions, organes ou organismes de l'Union, à l'exclusion de la Cour de justice de l'Union européenne dans l'exercice de ses fonctions juridictionnelles.

Article 44

Droit de pétition

Tout citoyen de l'Union ainsi que toute personne physique ou morale résidant ou ayant son siège statutaire dans un État membre a le droit de pétition devant le Parlement européen.

Article 45

Liberté de circulation et de séjour

1. Tout citoyen de l'Union a le droit de circuler et de séjourner librement sur le territoire des États membres.

2. La liberté de circulation et de séjour peut être accordée, conformément aux traités, aux ressortissants de pays tiers résidant légalement sur le territoire d'un État membre.

Article 46

Protection diplomatique et consulaire

Tout citoyen de l'Union bénéficie, sur le territoire d'un pays tiers où l'État membre dont il est ressortissant n'est pas représenté, de la protection des autorités diplomatiques et consulaires de tout État membre dans les mêmes conditions que les ressortissants de cet État.

TITRE VI : JUSTICE

Article 47

Droit à un recours effectif et à accéder à un tribunal impartial

Toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés a droit à un recours effectif devant un tribunal dans le respect des conditions prévues au présent article.

Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable par un tribunal indépendant et impartial, établi préalablement par la loi. Toute personne a la possibilité de se faire conseiller, défendre et représenter.

Une aide juridictionnelle est accordée à ceux qui ne disposent pas de ressources suffisantes, dans la mesure où cette aide serait nécessaire pour assurer l'effectivité de l'accès à la justice.

Article 48

Présomption d'innocence et droits de la défense

1. Tout accusé est présumé innocent jusqu'à ce que sa culpabilité ait été légalement établie.
2. Le respect des droits de la défense est garanti à tout accusé.

Article 49

Principes de légalité et de proportionnalité des délits et des peines

1. Nul ne peut être condamné pour une action ou une omission qui, au moment où elle a été commise, ne constituait pas une infraction d'après le droit national ou le droit international. De même, il n'est infligé aucune peine plus forte que celle qui était applicable au moment où l'infraction a été commise. Si, postérieurement à cette infraction, la loi prévoit une peine plus légère, celle-ci doit être appliquée.

2. Le présent article ne porte pas atteinte au jugement et à la punition d'une personne coupable d'une action ou d'une omission qui, au moment où elle a été commise, était criminelle d'après les principes généraux reconnus par l'ensemble des nations.

3. L'intensité des peines ne doit pas être disproportionnée par rapport à l'infraction.

Article 50

Droit à ne pas être jugé ou puni pénalement deux fois pour une même infraction

Nul ne peut être poursuivi ou puni pénalement en raison d'une infraction pour laquelle il a déjà été acquitté ou condamné dans l'Union par un jugement pénal définitif conformément à la loi.

TITRE VII : DISPOSITIONS GÉNÉRALES RÉGISSANT L'INTERPRÉTATION ET L'APPLICATION DE LA CHARTE

Article 51

Champ d'application

1. Les dispositions de la présente Charte s'adressent aux institutions, organes et organismes de l'Union dans le respect du principe de subsidiarité, ainsi qu'aux États membres uniquement lorsqu'ils mettent en œuvre le droit de l'Union. En conséquence, ils respectent les droits, observent les principes et en promeuvent l'application, conformément à leurs compétences respectives et dans le respect des limites des compétences de l'Union telles qu'elles lui sont conférées dans les traités.

2. La présente Charte n'étend pas le champ d'application du droit de l'Union au-delà des compétences de l'Union, ni ne crée aucune compétence ni aucune tâche nouvelles pour l'Union et ne modifie pas les compétences et tâches définies dans les traités.

Article 52

Portée et interprétation des droits et des principes

1. Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

2. Les droits reconnus par la présente Charte qui font l'objet de dispositions dans les traités s'exercent dans les conditions et limites définies par ceux-ci.

3. Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue.

4. Dans la mesure où la présente Charte reconnaît des droits fondamentaux tels qu'ils résultent des traditions constitutionnelles communes aux États membres, ces droits doivent être interprétés en harmonie avec lesdites traditions.

5. Les dispositions de la présente Charte qui contiennent des principes peuvent être mises en œuvre par des actes législatifs et exécutifs pris par les institutions, organes et organismes de l'Union, et par des actes des États membres lorsqu'ils mettent en œuvre le droit de l'Union, dans l'exercice de leurs compétences respectives. Leur invocation devant le juge n'est admise que pour l'interprétation et le contrôle de la légalité de tels actes.

6. Les législations et pratiques nationales doivent être pleinement prises en compte comme précisé dans la présente Charte.

7. Les explications élaborées en vue de guider l'interprétation de la présente Charte sont dûment prises en considération par les juridictions de l'Union et des États membres.

Article 53

Niveau de protection

Aucune disposition de la présente Charte ne doit être interprétée comme limitant ou portant atteinte aux droits de l'homme et libertés fondamentales reconnus, dans leur champ d'application respectif, par le droit de l'Union, le droit international et les conventions internationales auxquelles sont parties l'Union, ou tous les États membres, et notamment la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, ainsi que par les constitutions des États membres.

Article 54

Interdiction de l'abus de droit

Aucune des dispositions de la présente Charte ne doit être interprétée comme impliquant un droit quelconque de se livrer à une activité ou d'accomplir un acte visant à la destruction des droits ou libertés reconnus dans la présente Charte ou à des limitations plus amples des droits et libertés que celles qui sont prévues par la présente Charte.

*

* *

Le texte ci-dessus reprend, en l'adaptant, la Charte proclamée le 7 décembre 2000 et la remplacera à compter du jour de l'entrée en vigueur du traité de Lisbonne.

Annexe 3 : Index des risques VUE

Valeurs de l'UE	Droits fondamentaux de concrétisation	Mots-clefs
Dignité humaine	Dignité humaine	• Exploitation des vulnérabilités des personnes • Personne détenue • Personne retenue • Prestations sociales • Logement • Electricité • Télécommunications • Services d'urgence • Polygraphe • Evaluation du risque que représente une personne • Note sociale
	Droit à la vie	• Dispositif de sécurité • Equipements médicaux • Etranger • Armes • Peine de mort • Agents de l'Etat
	Droit à l'intégrité de la personne	• Dispositif de sécurité • Dispositif de sécurité de la gestion et de l'utilisation d'infrastructures critiques • Techniques subliminales • Interfaces cerveau-machine • Réalité virtuelle • Détection et reconnaissance des émotions • Manipulations génétiques • Neuro-technologies • Voix • Image des personnes

		• Hypertrucage • Enfant
Liberté	Respect de la vie privée et familiale	• Personne physique • Agents conversationnels (*chatbots*) • Robots assistants • Vidéosurveillance • Domicile • Domotique • Communications • Identification biométrique à distance en temps réel • Reconnaissance faciale
	Protection des données à caractère personnel	• Données à caractère personnel • Personne physique
Egalité	Droit à la non-discrimination	• Catégorisation biométrique • Age • Appartenance ethnique • Race • Couleur de peau • Sexe • Handicap • Caractéristiques génétiques • Corpulence • Démarche • Tenue vestimentaire • Accès aux services publics • Assurances • Travail • Orientation sexuelle • Education et formation
	Droits de l'enfant	• Enfant • Données à caractère personnel

	Droit d'intégration des personnes handicapées	• Personnes handicapées • Accès aux services publics • Education et formation

Annexe 4 : Tableau descriptif du SIA

Numéro	Explication	Question	Réponse
Personnes impliquées dans le cycle de vie du SIA			
1.	Une répartition claire des responsabilités (à différents niveaux) est essentielle pour garantir le développement et le déploiement d'un SIA respectueux des VUE. C'est en particulier le cas s'il existe des risques d'atteinte aux VUE. En effet, seule une répartition claire des responsabilités peut permettre l'adoption de mesures d'élimination ou d'atténuation des risques utiles. Pour répondre à cette question, il n'est pas nécessaire de désigner nommément l'ensemble des personnes impliquées. Il est en revanche important d'identifier les groupes de personnes amenées à participer au projet et de mentionner leurs responsabilités dans le projet	Quelles sont les personnes impliquées dans le projet et leurs responsabilités ? - Dans la conception ? - Dans la vérification et la validation ? - Dans le déploiement ? - Dans l'exploitation et le suivi ?	
La destination du SIA ou les finalités			

L'objectif de cette question est de dégager la destination du SIA et la ou les finalités pour lesquelles le SIA est développé. La description de la destination consiste à expliquer les besoins qu'il cherche à satisfaire. La destination du SIA est définie par le fournisseur. La description des finalités vise à expliquer les causes pour lesquelles le SIA est utilisé par le déployeur. Il s'agit de répondre à la question « pourquoi ? ». *Les finalités doivent être distinguées des fonctions du SIA. Les fonctions du SIA désignent les tâches ou les actions qu'il effectue afin de répondre aux besoins, d'atteindre les finalités pour lesquelles il a été développé. Alors que les finalités ont une raison d'être qui leur est propre, les fonctions du SIA ont une dimension fonctionnelle puisqu'elles servent un objectif, à savoir réaliser ces finalités.*			
2.	Il s'agit d'expliquer pourquoi le SIA a été développé, à quel besoin il répond (par ex., sécuriser un lieu, améliorer l'efficacité du processus productif). La réponse à cette question nécessite de connaître les besoins du déployeur[clxxxiv]. La difficulté provient du fait que le SIA peut être développé sans que les besoins du déployeur soient précisément connus. Dans ce cas, la destination[clxxxv] du SIA correspond aux finalités.	Quelles sont la destination ou les finalités du SIA ?	
3.	L'AI Act impose aux fournisseurs de prendre en compte la « mauvaise utilisation raisonnablement prévisible ». Il s'agit de « l'utilisation d'un système d'IA d'une manière qui n'est pas conforme à sa destination, mais qui peut résulter d'un comportement	Quelles sont les mauvaises utilisations raisonnablement prévisibles ?	

	humain raisonnablement prévisible ou d'une interaction raisonnablement prévisible avec d'autres systèmes, y compris d'autres systèmes d'IA » (AI Act, art. 3, §13).		
Les fonctions du SIA *Les fonctions du SIA sont les tâches que le SIA doit effectuer. Il faut distinguer, dans la mesure du possible, les fonctions et les finalités du SIA. En principe, les réponses aux questions relatives aux finalités et aux fonctions doivent être différentes.*			
4.	Il s'agit d'expliquer quels sont les résultats attendus, quelles tâches le SIA est appelé à effectuer pour répondre aux besoins du déployeur ou de l'utilisateur. La réponse doit être suffisamment précise, toutes les tâches et actions pouvant être opérées par le SIA devant figurer, mais il n'est pas nécessaire de détailler le fonctionnement de chacune de ces tâches et actions. Le fonctionnement précis doit être décrit dans les questions suivantes. Pour un SIA de réidentification de personnes ou d'objets par exemple, il s'agit de mentionner : Identification des personnes et d'objets ; Réidentification de la	Quelles sont les fonctions du SIA ?	

	personne ou de l'objet sur la base d'une requête par recherche de similarité.		
5.	Dans cette réponse, il faut indiquer si les tâches et actions qui doivent être effectuées par le SIA peuvent ou non être réalisées sans recours à l'IA. Il s'agit de justifier l'utilisation de l'IA c'est-à-dire d'expliquer pourquoi l'usage de l'IA est nécessaire. Néanmoins, il est possible que les tâches et actions peuvent être effectuées sans recours à l'IA. Il n'est pas obligatoire d'indiquer dans cette réponse que les tâches et actions ne peuvent pas être réalisées sans recours à l'IA. Si les tâches et actions peuvent être effectuées sans recours à l'IA, il faudra justifier la plus-value de l'usage d'un SIA dans la question suivante. Il convient par exemple d'expliquer que les tâches ou les actions peuvent être difficilement effectuées, voire ne peuvent pas l'être, par un humain ou par un système n'utilisant pas d'IA. Cette explication doit idéalement se baser	Est-ce que ces tâches peuvent être réalisées sans recours à un SIA ?	

	sur des études démontrant l'inefficacité de l'humain ou des systèmes sans IA.		
6.	La réponse à cette question a pour objectif de démontrer que le recours à l'IA présente un avantage par rapport au fonctionnement d'un système sans IA. Il faut prouver que l'usage de l'IA est pertinent, qu'il apporte une véritable plus-value. Il s'agit d'expliquer : - que le recours à l'IA est nécessaire pour accomplir la destination ou atteindre les finalités poursuivies, qui ne peuvent pas être réalisées sans recours à l'IA (cf. question précédente) ; ou - que l'usage de l'IA offre des avantages par rapport à un fonctionnement sans IA, c'est-à-dire que l'IA permet accomplir la destination ou atteindre les finalités poursuivies de façon plus efficace, notamment en termes de rapidité ou d'exactitude.	Quels sont les avantages du recours à l'IA ?	

	Cette démonstration doit être justifiée scientifiquement. Il faut démontrer par des études ou des tests l'efficacité du SIA par rapport à un système fonctionnant sans IA. Il s'agit de comparer le SIA aux capacités humaines ou de systèmes n'utilisant pas l'IA. Cette comparaison doit faire ressortir la plus grande efficacité du SIA, efficacité qui peut être entendue comme l'obtention d'un résultat plus rapidement ou plus exact. Il faut démontrer l'efficacité du SIA. Cette démonstration doit se fonder sur des études prouvant la meilleure efficacité du SIA. Si les actions ou tâches ne peuvent pas être réalisées par un humain ou par un système n'utilisant pas l'IA, on peut considérer, sans justification supplémentaire, que l'usage du SIA offre une plus-value.		
7.	La réponse à cette question doit permettre d'identifier les personnes ayant vocation à utiliser le SIA. Il s'agit de décrire ces personnes au regard de leurs qualités et de leurs	Qui sont les utilisateurs du SIA ?	

	compétences. La réponse à cette question permet, d'une part, d'évaluer le niveau des risques et, d'autre part, de déterminer les mesures de gestion des risques les plus appropriées. Il s'agit en premier lieu d'indiquer si l'utilisateur du SIA est un consommateur ou un professionnel. Les exigences en termes de compétence ne peuvent pas être les mêmes selon la qualité de consommateur ou de professionnel. Puis, en second lieu, le profil de l'utilisateur c'est-à-dire ses qualifications ou son expérience professionnelle.		
Les objets traités par le SIA *L'objectif de cette question est de dégager les catégories d'objets ou de personnes avec lesquels le SIA interagit. La réponse à cette question permet notamment d'identifier les enjeux juridiques liés aux VUE en interaction avec la cartographie.*			
8.	Pour répondre à cette question, il convient de mentionner les catégories de personnes ou d'objets auxquels les données traitées par le SIA sont relatives, c'est-à-dire les personnes et les objets concernés. Il ne s'agit pas de décrire précisément les données traitées par le SIA ou	Quels sont les objets ou les personnes concernés ?	

	son fonctionnement mais d'expliquer avec quels éléments de son environnement il interagit. La réponse doit être aussi détaillée que possible. Si la destination précise n'est pas connue, il convient tout de même de mentionner les catégories de personnes et d'objets qui pourraient être concernés. Il peut s'agir de : - Personnes physiques (il convient idéalement de préciser cette information : s'agit-il de visiteurs d'un lieu, d'usagers d'un service, etc.) ; - Données à caractère personnel ; - Données n'ayant pas un caractère personnel (il convient de préciser le type de données : des images, des données statistiques, etc.) - Objets physiques (véhicules, aéronefs, bagages, etc.).		
Le contexte de déploiement du SIA *Le SIA est intégré à un contexte qui peut être défini matériellement, spatialement et temporellement. L'espace et la temporalité caractérisant l'usage du SIA ont des conséquences sur les risques de préjudice pouvant être subis par les individus et la collectivité.*			

Les caractéristiques du contexte du SIA doivent également être prises en compte pour la détermination des mesures de gestion des risques adaptées. *Si le contexte ne peut pas être connu précisément, il convient de mentionner les usages prévisibles.* *Enfin, il est possible que le SIA n'interagisse pas directement avec l'environnement physique (par exemple, un SIA qui aurait pour objet de traiter uniquement des objets dématérialisés et qui ne produirait que des objets dématérialisées). Dans ce cas, il faut mentionner l'absence d'interaction et de prise en compte de l'environnement physique.*			
9.	Il s'agit de décrire les caractéristiques des matériels nécessaires au fonctionnement du SIA au regard de sa destination ou de sa finalité. Il peut par exemple s'agir de robots autonomes, d'ordinateurs ou encore de caméras.	Quelles sont les ressources matérielles nécessaire pour utiliser le SIA ?	
10.	Les caractéristiques spatiales de contexte du SIA ont trait aux particularités des lieux spécifiques dans lesquels le SIA est utilisé. Il convient de décrire ces lieux en mentionnant leurs caractéristiques au regard de l'accessibilité du public et de leur destination. Si l'accessibilité ou la destination du lieu ne sont pas précisément connus, il convient, au regard de la destination du SIA, d'envisager un large éventail de possibilités dans la	Dans quels lieux le SIA est-il utilisé ?	

	limite de la mauvaise utilisation raisonnablement prévisible[clxxxvi]. Il faut ainsi préciser les caractéristiques du lieu (espace accueillant du public, voie publique, lieu privé, entreprise, etc.). - Accessibilité : Il s'agit d'indiquer si c'est un lieu privé ou un lieu public[clxxxvii] : o Le lieu privé est défini comme un endroit qui n'est ouvert à personne sauf autorisation de celui qui l'occupe d'une manière permanente ou temporaire : domicile, chambre d'hôpital ou d'hôtel, locaux d'une entreprise, etc. o Le lieu public peut être défini comme un lieu dont l'accès est ouvert largement : voie publique, jardins publics, restaurants,		

	cinémas, magasins, etc. - Destination : La destination du lieu est l'usage qui en fait par les occupants : usage à titre de domicile, salle de repos, etc.		
11.	Il s'agit de décrire l'utilisation du SIA en termes temporel, si cela est pertinent. Il convient d'indiquer les moments d'utilisation du SIA, soit sur des plages horaires soit en lien avec des activités. Le SIA peut fonctionner en permanence ou à des heures spécifiques (par exemple la nuit ou durant les heures d'ouverture d'une entreprise).	A quels moments le SIA est-il utilisé ?	
La description technique du SIA *Les questions relatives aux technologies utilisées ont pour objet de détailler précisément le fonctionnement du SIA. Les questions sont notamment relatives aux méthodes d'IA utilisées et aux données. Les réponses permettent de déterminer le niveau de risque et les mesures de gestion de risque appropriées.*			
12.	Il convient de mentionner les caractéristiques des données d'entraînement[clxxxviii], de validation[clxxxix] et de test[cxc] et les raisons ayant conduit à choisir ce jeu de données et la source du jeu de données.	Quelles sont les données utilisées pour développer, entraîner, valider et tester le SIA ? Quelle est la source de ces données ?	

13.	Il s'agit d'indiquer les données utilisées par le SIA en phase de *run* lors de son utilisation[cxci]. Il convient de présenter les caractéristiques de ces données et leur source.	Quelles sont les données d'entrée traitées par le SIA lors de son fonctionnement ? Quelle est la source de ces données ?	
14.	La réponse à cette question consiste à détailler les différentes données produites par le SIA en fonctionnement. Il s'agit d'indiquer les décisions, entendu au sens large, que l'algorithme peut prendre comme une correspondance entre des objets, une décision relative à une personne, une action à effectuer, etc.	Quelles sont les données produites par le SIA lors de son fonctionnement ?	
15.	Il s'agit d'expliquer les techniques et approches d'IA utilisées (apprentissage automatique, etc.)	Quel est le type d'algorithme utilisé ?	
16.	Il convient de justifier le choix par rapport aux finalités et fonctions du SIA. En effet, certaines techniques et approches d'IA sont plus susceptibles de porter atteinte aux VUE que d'autres. Ainsi, il convient d'expliquer pourquoi ce choix a été fait, de justifier son utilisation par rapport à des techniques et	Pourquoi ce type d'algorithme a-t-il été choisi ?	

	approches qui pourraient se révéler plus respectueuses des VUE. Cette réponse doit idéalement être justifiée par des tests prouvant la meilleure efficacité du type d'algorithme choisi par rapport à d'autres pour réaliser les tâches et actions assignées au SIA.		
17.	Le niveau d'exactitude est un élément essentiel de la performance du SIA. Le niveau d'exactitude doit correspondre à celui établi par les normes techniques applicables au SIA, si elles existent. A défaut, l'exactitude doit garantir la performance du SIA.	Quel est le niveau d'exactitude du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ?	
18.	La robustesse permet de garantir la performance du SIA quel que soit le contexte de déploiement du SIA. Les exigences en termes de robustesse doivent correspondre à celles établies par les normes techniques applicables au SIA, si elles existent. A défaut, la robustesse doit garantir la performance du SIA.	Quel est le niveau de robustesse du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ?	
19.	La résilience doit permettre de garantir la performance du SIA	Quel est le niveau de résilience du SIA dans	

	malgré le changement de circonstances. Les exigences en termes de résilience doivent correspondre à celles établies par les normes techniques applicables au SIA, si elles existent. A défaut, la résilience doit garantir un niveau suffisant de performance du SIA.	des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ?	
20.	La cybersécurité est un élément essentiel pour garantir la performance du SIA et éviter les atteintes aux personnes et aux biens pouvant résulter d'actes de malveillance. Les exigences en termes de cybersécurité doivent correspondre à celles établies par les normes techniques applicables au SIA, si elles existent. A défaut, la cybersécurité doit garantir un niveau suffisant de performance du SIA.	Quel est le niveau de cybersécurité du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ?	
La description scalaire du fonctionnement du SIA *Ces questions ont pour but de donner l'ordre de grandeur projeté du déploiement du SIA. La détermination de cet ordre de grandeur est essentielle notamment pour établir l'ampleur du préjudice pouvant résulter de l'utilisation du SIA, ce qui a des conséquences directes sur le niveau de risque et donc l'acceptabilité de ce risque.* *La difficulté provient du fait que l'importance du déploiement d'un point de vue géographique, temporel ou numérique n'est pas nécessairement connue lors du développement du SIA. Dans ce cas, les réponses ne peuvent être qu'hypothétiques ou alors être une mention des capacités maximales du SIA. Dans tous les cas, il convient de prendre en compte la destination du SIA.*			

21.	Il convient de décrire la zone de déploiement du SIA. Il peut s'agir d'une échelle : - Locale (lieu spécifique, ville ou territoire peu étendu comme un département ou une région français) - Régionale (une grande partie d'un territoire national, un pays ou un groupe de pays) - Internationale (Union européenne, de nombreux pays à travers le monde voire le monde entier)	A quelle échelle géographique le SIA est-il utilisé ?	
22.	Il s'agit d'indiquer la durée de déploiement du SIA. La durée peut être déterminée, si une date de fin de mise en service est prévue, ou indéterminée. La réponse dépend des modalités d'exploitation et de suivi prévue et notamment d'un éventuel accord contractuel avec le déployeur.	A quelle échelle temporelle le SIA est-il utilisé ?	
23.	Il faut décrire la nombre de personnes ou d'objets qui peuvent être concernés par le SIA. Il convient d'indiquer sur une plage horaire, par exemple sur 24 heures	A quelle échelle en termes d'objets le SIA est-il utilisé ?	

	si le SIA fonctionne en continu ou durant sa durée d'utilisation spécifique, combien de personnes ou d'objets (qu'il s'agisse de véhicules ou de données à caractère personnel par exemple) peuvent être concernés par le SIA. Il peut par exemple s'agir de centaines voire de milliers de passagers dans une gare ou de véhicules sur une route ou encore des milliers de données à caractère personnel. La question à cette réponse est notamment décisive pour déterminer s'il y a une utilisation du SIA à grande échelle.		

[clxxxiv] Le déployeur est une personne physique ou morale, une autorité publique, une agence ou un autre organisme utilisant sous sa propre autorité un système d'IA sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel (AI Act, art. 3, §4).

[clxxxv] La destination du SIA est l'utilisation à laquelle un système d'IA est destiné par le fournisseur, y compris le contexte et les conditions spécifiques d'utilisation, tels qu'ils sont précisés dans les informations communiquées par le fournisseur dans la notice d'utilisation, les indications publicitaires ou de vente et les déclarations, ainsi que dans la documentation technique (AI Act, art. 3, §12).

[clxxxvi] La mauvaise utilisation raisonnablement prévisible est l'utilisation d'un système d'IA d'une manière qui n'est pas conforme à sa destination, mais qui peut résulter d'un comportement humain raisonnablement prévisible ou d'une interaction raisonnablement prévisible avec d'autres systèmes, y compris d'autres systèmes d'IA (AI Act, art. 3, §13).

[clxxxvii] L'AI Act emploie l'expression d' « espace accessible au public ». Il s'agit de « tout espace physique accessible à un nombre indéterminé de personnes physiques, que l'espace en question soit privé ou public, et indépendamment de l'activité pour laquelle il peut être utilisé, comme pour le commerce, par exemple, magasins, restaurants ou cafés, pour la prestation de services, par exemple, banques, activités professionnelles ou hôtellerie, pour la pratique de sports, par exemple, piscines, salles de sport ou stades, pour les transports, par exemple, gares routières, stations de métro et gares ferroviaires, aéroports ou moyens de transport, pour les divertissements, par exemple, cinémas, théâtres, musées, salles de concert et de conférence, ou pour les loisirs ou autres, par exemple, routes et places publiques, parcs, forêts ou terrains de jeux. Un espace devrait également être classé comme accessible au public si, indépendamment de la capacité potentielle ou des restrictions de sécurité, l'accès est soumis à certaines conditions

prédéterminées qui peuvent être remplies par un nombre indéterminé de personnes, telles que l'achat d'un billet ou d'un titre de transport, l'enregistrement préalable ou le fait d'avoir un certain âge. En revanche, un espace ne devrait pas être considéré comme étant accessible au public si l'accès est limité à certaines personnes physiques, définies soit par le droit de l'Union soit par le droit national directement lié à la sûreté ou à la sécurité publiques, ou par la manifestation claire de la volonté de la personne disposant de l'autorité compétente sur l'espace. Le seul fait d'avoir une possibilité d'accès, comme une porte déverrouillée ou une porte ouverte dans une clôture, n'implique pas que l'espace est accessible au public en présence d'indications ou de circonstances suggérant le contraire, comme des signes d'interdiction ou de restriction d'accès. Les locaux des entreprises et des usines, ainsi que les bureaux et les lieux de travail qui sont destinés à être accessibles uniquement aux employés et prestataires de services concernés ne sont pas des espaces accessibles au public. Les espaces accessibles au public ne devraient pas inclure les prisons ni le contrôle aux frontières. D'autres espaces peuvent comprendre à la fois des espaces accessibles au public et des espaces non accessibles au public, comme le hall d'un bâtiment d'habitation privé par lequel il faut passer pour accéder au bureau d'un médecin ou le hall d'un aéroport. Les espaces en ligne ne sont pas couverts, car ce ne sont pas des espaces physiques. Le caractère accessible ou non au public d'un espace donné devrait cependant être déterminé au cas par cas, en tenant compte des particularités de la situation en question » (cons. 19).

[clxxxviii] Les données d'entraînement sont les données utilisées pour entraîner un système d'IA en ajustant ses paramètres entraînables (AI Act, art. 3, §29).

[clxxxix] Les données de validation sont les données utilisées pour fournir une évaluation du système d'IA entraîné et pour régler ses paramètres non entraînables ainsi que son processus d'apprentissage, afin, notamment, d'éviter tout sous-ajustement ou surajustement (AI Act., art. 3, §30).

[cxc] Les données de test sont les données utilisées pour fournir une évaluation indépendante du système d'IA afin de confirmer la performance attendue de ce système avant sa mise sur le marché ou sa mise en service (AI Act, art. 3, §32).

[cxci] Les données d'entrée sont les données fournies à un système d'IA ou directement acquises par celui-ci et à partir desquelles il produit une sortie (AI Act, art. 3, §33).

Annexe 5 : Fiche-Risques VUE

Risque n°1 :

1. Détermination du niveau de risque

A. Description du risque

N°	Question	Réponse
1)	Quel est le facteur de risque que présente le SIA ? *[reporter les mots-clefs de l'Index des risques VUE]*	
2)	Quelles sont les valeurs de l'Union européenne potentiellement menacées ? *[se reporter à l'Index des risques VUE]*	
3)	Quels sont le ou les préjudices potentiels ?	

Le facteur de risque, la VUE et le ou les préjudices doivent être mentionnés dans le Tableau synthétique de l'étude d'impact.

B. Niveau du risque

a) Sévérité du préjudice

1/ Conséquences :

N°	Question	Réponse
4)	Quelles sont les victimes potentielles ?	
5)	Quelles sont la nature et l'importance du ou des préjudices ?	
6)	Quel effort est nécessaire pour faire cesser ou réparer le ou les préjudices ?	
7)	Des dispositifs d'enregistrement conformes à l'article 12 de l'AI Act sont-ils prévus ?	

- Niveau des conséquences :

Au regard des caractéristiques des personnes concernées, de la nature et de l'importance des préjudices et de l'effort nécessaire pour faire cesser et réparer le préjudice, le niveau des conséquences peut être évalué à un niveau :

☐Faibles (1) ; ☐Modérées (2) ; ☐Importantes (3).

2/ Ampleur :

N°	Question	Réponse
8)	Quel est le nombre de victimes potentielles ?	
9)	Quelle est la criticité du secteur ?	

- Niveau de l'ampleur :

Au regard du nombre de personnes concernées et de la criticité du secteur, le niveau de l'ampleur peut être évalué à un niveau :

☐Individuelle (1) ; ☐Sectorielle (2) ; ☐Systémique (3).

3/ Evaluation de la sévérité du préjudice :

- Niveau des conséquences : *[reporter le niveau des conséquences]* : ☐Faibles (1) ; ☐Modérées (2) ; ☐Importantes (3).
- Niveau de l'ampleur : *[reporter le niveau de l'ampleur]* : ☐Individuelle (1) ; ☐Sectorielle (2) ; ☐Systémique (3).

Conséquences*Ampleur	Niveau de sévérité
1 ou 2	Faible/1
3 ou 4	Modérée/2
6 ou 9	Importante/3

La combinaison des critères des conséquences et de l'ampleur du ou des préjudices aboutissent à un niveau de sévérité : ☐Faible (1) ; ☐Modéré (2) ; ☐Important (3).

b) <u>Probabilité du préjudice</u>

N°	Question	Réponse
10)	Quel est le niveau d'exactitude du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau d'exactitude est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ? *[se reporter à la ques. 17 du Tableau descriptif]*	

11)	Quel est le niveau de robustesse du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de robustesse est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ? *[se reporter à la ques. 18 du Tableau descriptif]*	
12)	Quel est le niveau de résilience du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de résilience est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ? *[se reporter à la ques. 19 du Tableau descriptif]*	
13)	Quel est le niveau de cybersécurité du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de cybersécurité est-il conforme à l'état de l'art, tel qu'il	

	ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ? *[se reporter à la ques. 20 du Tableau descriptif]*	
14)	Les jeux de données d'entraînement, de validation et de test font-ils l'objet de pratiques de gouvernance et de gestion des données conformes aux dispositions de l'article 10, §2 de l'AI Act ? *[se reporter à la ques. 21 du Tableau descriptif]*	
15)	Les jeux de données d'entraînement, de validation et de test sont-ils pertinents, suffisamment représentatifs et, dans toute la mesure possible, exempts d'erreurs et complets au regard de la destination, conformément aux dispositions de l'article 10, §3 de l'AI Act ? Présentent-ils les propriétés statistiques appropriées, y compris, le cas échéant, en ce qui concerne les personnes ou groupes de personnes à l'égard desquels le SIA est destiné à être utilisé, conformément aux dispositions de l'article 10, §3 de l'AI Act ? *[se reporter à la ques. 12 du Tableau descriptif]*	

16)	Les jeux de données d'entraînement, de validation et de test tiennent-ils compte, dans la mesure requise par la destination, des caractéristiques ou éléments propres au cadre géographique, contextuel, comportemental ou fonctionnel spécifique dans lequel le SIA est destiné à être utilisé, conformément aux dispositions de l'article 10, §4 de l'AI Act ? *[se reporter à la ques. 12 du Tableau descriptif]*	
17)	Est-il prévu de mentionner dans la notice d'utilisation les informations suivantes, conformément aux dispositions de l'article 13 de l'AI Act : - la destination du SIA ; - le niveau d'exactitude, y compris les indicateurs utilisés, de robustesse et de cybersécurité qui a servi de référence pour les tests et la validation du SIA et qui peut être attendu, ainsi que toutes circonstances connues et prévisibles susceptibles d'avoir une incidence sur le niveau	

	attendu d'exactitude, de robustesse et de cybersécurité ; - le cas échéant, la performance du SIA en ce qui concerne des personnes ou groupes de personnes spécifiques à l'égard desquels le système est destiné à être utilisé ; - et les ressources informatiques et matérielles nécessaires, la durée de vie attendue du SIA et toutes les mesures de maintenance et de suivi, y compris leur fréquence, nécessaires pour assurer le bon fonctionnement du SIA, notamment en ce qui concerne les mises à jour logicielles ?	
18)	Quelles sont les mesures de contrôle humain mises en place, conformément aux dispositions de l'article 14 de l'AI Act ? De quelle façon permettent-elles de réduire la probabilité de survenance du préjudice ?	

- Niveau de probabilité :

Au regard des caractéristiques techniques du SIA et du respect des exigences essentielles de l'AI Act, le niveau de probabilité peut être évalué à un niveau :

☐Faible (1) ; ☐Modérée (2) ; ☐Importante (3).

c) Niveau du risque

- Niveau de sévérité : *[reporter le niveau de sévérité]* : ☐Faible (1) ; ☐Modéré (2) ; ☐Important (3).
- Niveau de probabilité : *[reporter le niveau de probabilité]* : ☐Faible (1) ; ☐Modérée (2) ; ☐Importante (3).
- Niveau du risque :

		Probabilité		
		1	2	3
Sévérité	1	1	2	3
	2	2	4	6
	3	3	6	9

La combinaison des critères de la sévérité et de la probabilité du ou des préjudices aboutissent à un niveau de risque :

☐Faible (1 ou 2) :

Dans ce cas, il n'est pas nécessaire de prendre des mesures de gestion du risque spécifiques à ce risque et il convient de se reporter directement à la partie « 3. Bilan » et *de mentionner dans le Tableau synthétique de l'étude d'impact que le niveau de risque est faible et acceptable dans la colonne Bilan*.

☐Modéré (3 ou 4) :

Dans ce cas, il convient de se reporter à la partie « 2. Contrôle de la proportionnalité » et *de mentionner dans le Tableau synthétique de l'étude d'impact que le niveau de risque est modéré*.

☐Important (6 ou 9) :

Dans ce cas, le risque est présumé disproportionné. Il convient alors de de se reporter directement à la *Fiche-Gestion risque VUE* et *de mentionner dans le Tableau synthétique de l'étude d'impact que le niveau de risque est important*.

Le niveau de risque doit être mentionné dans le Tableau synthétique de l'étude d'impact.

2. Contrôle de la proportionnalité

A. Critère de la nécessité

N°	Question	Réponse
19)	Quelle est la destination ou la finalité poursuivie ? *[se reporter à la ques. 2 du Tableau descriptif]*	
20)	Le recours aux technologies d'IA offre-t-il des avantages significatifs ? Indiquez précisément pour chaque fonction du SIA la plus-value qu'apporte l'IA *[se reporter aux ques. 5 et 6 du Tableau descriptif]*	*Réponse argumentée :* ☐Pour toutes les fonctions du SIA, le recours aux technologies d'IA offre des avantages significatifs. ☐Pour toutes les fonctions du SIA, e recours aux technologies d'IA n'offre pas d'avantages significatifs.
21)	Les conditions de déploiement du SIA (lieux et plages horaires d'utilisation) sont-elles nécessaires pour la mise en œuvre de la destination ou de la finalité poursuivie ? Justifiez ce caractère nécessaire *[se reporter aux ques. 10 et 11 du Tableau descriptif]* :	*Réponse argumentée :* ☐Les conditions de déploiement du SIA correspondent à ce qui est nécessaire pour atteindre la finalité poursuivie. ☐Les conditions de déploiement du SIA ne correspondent pas à ce qui est nécessaire pour atteindre la finalité poursuivie.
22)	L'échelle d'utilisation du SIA est-elle nécessaire pour la mise en œuvre de la destination ou de la finalité poursuivie ? Justifiez ce caractère nécessaire *[se*	*Réponse argumentée :* ☐L'échelle d'utilisation du SIA correspond à ce qui est nécessaire pour atteindre la finalité poursuivie.

	reporter aux ques. 21 et s. du Tableau descriptif] :	☐L'échelle d'utilisation du SIA ne correspond pas à ce qui est nécessaire pour atteindre la finalité poursuivie.

- Conclusion :

☐La mise en œuvre du SIA est nécessaire.

☐La mise en œuvre du SIA n'est pas nécessaire car :

☐Pour toutes les fonctions du SIA, le recours aux technologies d'IA n'offre pas d'avantages significatifs ;

☐Les conditions de déploiement ne correspondent pas à ce qui est nécessaire pour atteindre la destination ou finalité poursuivie ;

☐L'échelle d'utilisation du SIA ne correspond pas à ce qui est nécessaire pour atteindre la destination ou la finalité poursuivie.

B. Critère de la proportionnalité *stricto sensu*

N°	Question	Réponse
23)	Quelle est la destination ou la finalité poursuivie ? *[se reporter à la ques. 2 du Tableau descriptif]*	
24)	Quelle est la nature des intérêts poursuivis par la destination ou par le déployeur du SIA et lesquels sont-ils ? *[précisez s'il s'agit de droits et principes fondamentaux, et lesquels, ou d'autres intérêts, tel un intérêt commercial par exemple. V. Annexe 2 : Charte des droits fondamentaux de l'Union européenne)*	

- Conclusion

Au regard de la nature des intérêts poursuivis par la destination ou le déployeur, le risque paraît :

☐Proportionné car il s'agit d'un intérêt général, la mise en œuvre du SIA est donc proportionnée.

☐Disproportionné car il s'agit d'un intérêt particulier, la mise en œuvre du SIA est donc disproportionnée.

C. Conclusion du contrôle de la proportionnalité

☐La mise en œuvre du SIA est nécessaire ET proportionnée *stricto sensu*. Le risque est donc acceptable et aucune mesure de gestion de ce risque n'est requise. Il convient de se reporter ensuite à la partie « 3. Bilan » et *de mentionner dans le Tableau synthétique de l'étude d'impact que la mise en œuvre du SIA est proportionnée*.

☐La mise en œuvre du SIA n'est pas nécessaire ET proportionnée *stricto sensu*. Le risque est donc inacceptable et il convient de mettre en place des mesures de gestion de ce risque. Il convient pour ce faire de se reporter à la *Fiche-Gestion risques VUE*.

Plus précisément, font défaut le ou les caractères : ☐nécessaire ; ☐proportionné *stricto sensu*. Il convient *de mentionner dans le Tableau synthétique de l'étude d'impact que la mise en œuvre du SIA est disproportionnée et la source de la disproportion*.

Le caractère proportionné ou disproportionné doit être mentionné dans le Tableau synthétique de l'étude d'impact.

3. Bilan

Trois situations doivent être distinguées :

Niveau de risque	Bilan
Le risque d'atteinte aux VUE est faible	Dans ce cas, le risque est présumé proportionné et acceptable. Il convient de mentionner l'acceptabilité du risque dans le *Tableau synthétique de l'étude d'impact*. Il n'est pas nécessaire de prendre des mesures de gestion de ce risque.

Le risque d'atteinte aux VUE est <u>modéré</u>	<u>Risque proportionné et acceptable :</u> Le contrôle de la proportionnalité a permis de conclure que le niveau de risque est proportionné et donc acceptable. Dans ce cas, il convient de mentionner l'acceptabilité du risque dans le *Tableau synthétique de l'étude d'impact dans la colonne Bilan*. Il n'est pas nécessaire de prendre des mesures de gestion de ce risque.
	<u>Risque disproportionné et inacceptable :</u> Le contrôle de la proportionnalité a permis de conclure que le niveau de risque est disproportionné et donc inacceptable. Dans ce cas, les mesures de gestion de risque adoptées (Fiche-gestion risque VUE) doivent permettre d'éliminer le risque ou de réduire la sévérité ou la probabilité du préjudice ou de corriger les défauts liés à la nécessité et à la proportionnalité. Il convient alors de réaliser le bilan de l'étude d'impact. Le bilan consiste à réévaluer le niveau du risque et la proportionnalité du SIA en tenant compte des mesures de gestion des risques identifiées. Deux situations peuvent se présenter : - Si le risque a été éliminé par les mesures de gestion des risques, dans ce cas, il faut considérer que le bilan de l'étude d'impact est positif. Il ne faut pas réévaluer le niveau du risque, puisque ce dernier a été éliminé, ni réévaluer la proportionnalité. - Si le risque n'a pas pu être éliminé, dans ce cas il faut évaluer l'effet des mesures de gestion du risque. A cette fin, il convient de reprendre les points suivants en modifiant les réponses afin de prendre en compte les mesures de gestion du risque : o 1. B. Niveau de risque o 2. Contrôle de la proportionnalité. A cette fin, un tableau est présenté ci-après. A l'issue de cette réévaluation, il faut noter les effets des mesures de gestion des risques et préciser si le risque est devenu ou non acceptable. Il convient de noter le résultat dans la colonne Bilan du *Tableau synthétique de l'étude d'impact*.
Le risque d'atteinte aux VUE est <u>important</u>	Le risque est présumé disproportionné et donc inacceptable. Le contrôle de la proportionnalité a permis de conclure que le niveau de risque est disproportionné et donc inacceptable. Dans ce cas, les mesures de gestion de risque adoptées (Fiche-gestion risque VUE) doivent permettre d'éliminer le risque

	ou de réduire la sévérité ou la probabilité du préjudice ou de corriger les défauts liés à la nécessité et à la proportionnalité. Il convient alors de réaliser le bilan de l'étude d'impact. Le bilan consiste à réévaluer le niveau du risque et la proportionnalité du SIA en tenant compte des mesures de gestion des risques identifiées. Deux situations peuvent se présenter : - Si le risque a été éliminé par les mesures de gestion des risques, dans ce cas, il faut considérer que le bilan de l'étude d'impact est positif. Il ne faut pas réévaluer le niveau du risque, puisque ce dernier a été éliminé, ni réévaluer la proportionnalité. - Si le risque n'a pas pu être éliminé, dans ce cas il faut évaluer l'effet des mesures de gestion du risque. A cette fin, il convient de reprendre les points suivants en modifiant les réponses afin de prendre en compte les mesures de gestion du risque : o 1. B. Niveau de risque o 2. Contrôle de la proportionnalité. A cette fin, un tableau est présenté ci-après. A l'issue de cette réévaluation, il faut noter les effets des mesures de gestion des risques et préciser si le risque est devenu ou non acceptable. Il convient de noter le résultat dans la colonne Bilan du *Tableau synthétique de l'étude d'impact*.

Le tableau suivant reprend les questions des parties précédentes. Il est possible de ne répondre qu'aux seules questions affectées par les mesures de gestion du risques adoptées.

Question	Réponse
<u>Niveau de risque</u>	
Quels sont le ou les préjudices potentiels ?	
Sévérité du préjudice	
Quelles sont les victimes potentielles ?	

Question	Réponse
Quelles sont la nature et l'importance du ou des préjudices ?	
Quel effort est nécessaire pour faire cesser ou réparer le ou les préjudices ?	
Des dispositifs d'enregistrement conformes à l'article 12 de l'AI Act sont-ils prévus ?	
Au regard des caractéristiques des personnes concernées, de la nature et de l'importance des préjudices et de l'effort nécessaire pour faire cesser et réparer le préjudice, le niveau des conséquences peut être évalué à un niveau :	☐Faibles (1) ; ☐Modérées (2) ; ☐Importantes (3).
Quel est le nombre de victimes potentielles ?	
Quelle est la criticité du secteur ?	
Au regard du nombre de personnes concernées et de la criticité du secteur, le niveau de l'ampleur peut être évalué à un niveau :	☐Individuelle (1) ; ☐Sectorielle (2) ; ☐Systémique (3).
La combinaison des critères des conséquences et de l'ampleur du ou des préjudices aboutissent à un niveau de sévérité :	☐Faible (1) ; ☐Modéré (2) ; ☐Important (3).
Probabilité du préjudice	

Question	Réponse
Quel est le niveau d'exactitude du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau d'exactitude est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ?	
Quel est le niveau de robustesse du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de robustesse est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ?	
Quel est le niveau de résilience du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de résilience est-il conforme à l'état de l'art, tel qu'il ressort notamment de	

Question	Réponse
l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ?	
Quel est le niveau de cybersécurité du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de cybersécurité est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ?	
Les jeux de données d'entraînement, de validation et de test font-ils l'objet de pratiques de gouvernance et de gestion des données conformes aux dispositions de l'article 10, §2 de l'AI Act ?	
Les jeux de données d'entraînement, de validation et de test sont-ils pertinents, suffisamment représentatifs et, dans toute la mesure possible, exempts d'erreurs et complets au regard de la destination, conformément aux dispositions de l'article 10, §3 de l'AI Act ?	

Question	Réponse
Présentent-ils les propriétés statistiques appropriées, y compris, le cas échéant, en ce qui concerne les personnes ou groupes de personnes à l'égard desquels le SIA est destiné à être utilisé, conformément aux dispositions de l'article 10, §3 de l'AI Act ?	
Les jeux de données d'entraînement, de validation et de test tiennent-ils compte, dans la mesure requise par la destination, des caractéristiques ou éléments propres au cadre géographique, contextuel, comportemental ou fonctionnel spécifique dans lequel le SIA est destiné à être utilisé, conformément aux dispositions de l'article 10, §4 de l'AI Act ?	
Est-il prévu de mentionner dans la notice d'utilisation les informations suivantes, conformément aux dispositions de l'article 13 de l'AI Act : **- la destination du SIA ;** **- le niveau d'exactitude, y compris les indicateurs**	

Question	Réponse
utilisés, de robustesse et de cybersécurité qui a servi de référence pour les tests et la validation du SIA et qui peut être attendu, ainsi que toutes circonstances connues et prévisibles susceptibles d'avoir une incidence sur le niveau attendu d'exactitude, de robustesse et de cybersécurité ; - **le cas échéant, la performance du SIA en ce qui concerne des personnes ou groupes de personnes spécifiques à l'égard desquels le système est destiné à être utilisé ;** - **et les ressources informatiques et matérielles nécessaires, la durée de vie attendue du SIA et toutes les mesures de maintenance et de suivi, y compris leur fréquence, nécessaires pour assurer le bon fonctionnement du SIA, notamment en ce qui**	

Question	Réponse
concerne les mises à jour logicielles ?	
Quelles sont les mesures de contrôle humain mises en place, conformément aux dispositions de l'article 14 de l'AI Act ? De quelle façon permettent-elles de réduire la probabilité de survenance du préjudice ?	
Au regard des caractéristiques techniques du SIA et du respect des exigences essentielles de l'AI Act, le niveau de probabilité peut être évalué à un niveau :	☐Faible (1) ; ☐Modérée (2) ; ☐Importante (3).
Niveau du risque : conclusion	
La combinaison des critères de la sévérité et de la probabilité du ou des préjudices aboutissent à un niveau de risque :	☐Faible (1 ou 2) ; ☐Modéré (3 ou 4) ; ☐Important (6 ou 9).
<u>Contrôle de la proportionnalité</u>	
Critère de la nécessité	
Quelle est la destination ou la finalité poursuivie ?	
Le recours aux technologies d'IA offre-t-il des avantages significatifs ? Indiquez précisément pour chaque fonction du SIA la plus-value	*Réponse argumentée :*

Question	Réponse
qu'apporte l'IA ***[se reporter aux ques. 5 et 6 du Tableau descriptif]***	☐Pour toutes les fonctions du SIA, le recours aux technologies d'IA offre des avantages significatifs. ☐Pour toutes les fonctions du SIA, e recours aux technologies d'IA n'offre pas d'avantages significatifs.
Les conditions de déploiement du SIA (lieux et plages horaires d'utilisation) sont-elles nécessaires pour la mise en œuvre de la destination ou de la finalité poursuivie ? Justifiez ce caractère nécessaire ***[se reporter aux ques. 10 et 11 du Tableau descriptif]*** **:**	*Réponse argumentée :* ☐Les conditions de déploiement du SIA correspondent à ce qui est nécessaire pour atteindre la finalité poursuivie. ☐Les conditions de déploiement du SIA ne correspondent pas à ce qui est nécessaire pour atteindre la finalité poursuivie.
L'échelle d'utilisation du SIA est-elle nécessaire pour la mise en œuvre de la destination ou de la finalité poursuivie ? Justifiez ce caractère nécessaire ***[se reporter aux ques. 21 et s. du Tableau descriptif]*** **:**	*Réponse argumentée :* ☐L'échelle d'utilisation du SIA correspond à ce qui est nécessaire pour atteindre la finalité poursuivie. ☐L'échelle d'utilisation du SIA ne correspond pas à ce qui est nécessaire pour atteindre la finalité poursuivie.
Critère de la proportionnalité *stricto sensu*	
Quelle est la destination ou la finalité poursuivie ? ***[se reporter à la ques. 2 du Tableau descriptif]***	
Quelle est la nature des intérêts poursuivis par la destination ou par le déployeur du SIA et lesquels sont-ils ? ***[précisez s'il s'agit de droits et principes fondamentaux, et lesquels,***	

Question	Réponse
ou d'autres intérêts, tel un intérêt commercial par exemple]	

- Conclusion de la réévaluation du niveau de risque et de la proportionnalité

A l'issue de cette réévaluation du niveau de risque et de la proportionnalité, le risque paraît :

☐Acceptable ;

☐Inacceptable.

Si le risque demeure inacceptable, il convient de repenser la conception et le développement du SIA puis de réaliser de nouveau une étude d'impact jusqu'à ce que le risque puisse être considéré comme acceptable.

Le résultat final doit être reporté dans la colonne finale du Tableau synthétique de l'étude d'impact.

Annexe 6 : Fiche-Gestion risques VUE

Risque n°1 :

1. Mesures de gestion du risque

A. Si la mise en œuvre du SIA n'est pas nécessaire

a) Si le recours aux technologies d'IA n'offre pas d'avantages significatifs

- Objectif des mesures de gestion du risque

L'objectif des mesures de gestion de ce risque consiste à garantir un recours aux technologies d'IA mélioratif. Ainsi, les mesures de gestion de ce risque vise à limiter l'usage de l'IA aux fonctions pour lesquelles l'IA présente une efficacité accrue par rapport à la réalisation de ces mêmes actions sans recours à l'IA.

- Identification des mesures de gestion du risque adaptées

N°	Question	Réponse
1)	Les fonctions n'offrant pas d'avantages significatifs peuvent-elles être supprimées sans porter atteinte à la performance du SIA ni nuire à la possibilité pour le SIA d'atteindre la finalité poursuivie ?	☐Si oui, lesquelles ? La suppression de ces fonctions constitue une mesure de gestion de ce risque. *Réponse :* ☐Si non, il convient de reconsidérer la conception et le développement du SIA au regard de la destination et de la finalité poursuivie.

Conclusion :

Quelles sont les mesures de gestion du risque pouvant être adoptées en réponse à ce problème ?

Ces mesures de gestion du risque doivent être reportées dans le Tableau synthétique de l'étude d'impact.

b) Si les conditions de déploiement ne correspondent pas à ce qui est nécessaire pour atteindre la finalité poursuivie

- Objectif des mesures de gestion du risque

L'objectif des mesures de gestion de ce risque est d'accorder les conditions de déploiement du SIA à ce qui est nécessaire pour atteindre la destination ou la finalité poursuivie. Il convient à cette fin de redéfinir les conditions de déploiement du SIA.

- Identification des mesures de gestion du risque adaptées

N°	Question	Réponse
2)	Les conditions de déploiement ont-elles été définies par rapport à la destination ou la finalité poursuivie ?	☐Si oui, il convient de réviser les conditions de déploiement par rapport à la destination ou à la finalité poursuivie. Il convient ensuite de se reporter à la question suivante. ☐Si non, la révision des conditions de déploiement au regard de la finalité poursuivie constitue une mesure de gestion de ce risque.
3)	Est-il possible modifier les conditions de déploiement du SIA sans porter atteinte à la performance du SIA ou à la possibilité de réaliser la finalité poursuivie ?	☐Si oui, la modification des conditions de déploiement constitue une mesure de gestion des risques. ☐Si non, il convient de reconsidérer la conception et le développement du SIA au regard de la destination ou de la finalité poursuivie.

Conclusion :

Quelles sont les mesures de gestion du risque pouvant être adoptées en réponse à ce problème ?

Ces mesures de gestion du risque doivent être reportées dans le Tableau synthétique de l'étude d'impact.

c) Si l'échelle d'utilisation du SIA ne correspond pas à ce qui est nécessaire pour atteindre la destination ou la finalité poursuivie

- Objectif des mesures de gestion du risque

L'objectif des mesures de gestion de ce risque est de limiter l'échelle d'utilisation à une mesure n'outrepassant pas ce qui est nécessaire pour atteindre la destination ou la finalité poursuivie.

- Identification des mesures de gestion du risque adaptées

N°	Question	Réponse
4)	L'échelle d'utilisation a-t-elle été déterminée au regard de la destination ou de la finalité poursuivie ?	☐Si oui, il convient de reconsidérer l'adéquation entre l'échelle d'utilisation et la destination et la finalité poursuivie. Pour ce faire, il faut appliquer un principe de « minimisation » de l'utilisation des SIA, selon le problème que pose le SIA au regard du caractère nécessaire. ☐Si non, la réévaluation de l'échelle d'utilisation par rapport à la destination ou à la finalité poursuivie constitue une mesure de gestion de ce risque.

Conclusion :

Quelles sont les mesures de gestion du risque pouvant être adoptées en réponse à ce problème ?

Ces mesures de gestion du risque doivent être reportées dans le Tableau synthétique de l'étude d'impact.

B. Si la mise en œuvre du SIA n'est pas proportionnée *stricto sensu*

- Objectif des mesures de gestion du risque

L'objectif des mesures de gestion de ce risque est :
- D'éliminer le risque de préjudice portant atteinte aux VUE ; ou
- De diminuer la gravité ou la probabilité du ou des préjudices afin que le risque puisse être considéré comme proportionné.

a) Elimination du risque de préjudice

N°	Question	Réponse
5)	Le risque de préjudice peut-il être éliminé sans porter atteinte à la performance du SIA ou à la réalisation de la finalité poursuivie ?	☐Si oui, les mesures permettant d'éliminer ce risque constituent des mesures de gestion de ce risque. Il convient ensuite de se reporter directement à la partie « 3. Bilan » de la Fiche-Risques VUE. Précisez les mesures pouvant être prises pour éliminer ce risque. ☐Si non, il convient de se reporter à la partie suivante « b) Réduction du risque de préjudice ».

Conclusion :
Quelles sont les mesures de gestion du risque pouvant être adoptées en réponse à ce problème ?

Ces mesures de gestion du risque doivent être reportées dans le Tableau synthétique de l'étude d'impact.

b) Réduction du risque de préjudice

- Objectif des mesures de gestion du risque

L'objectif des mesures de gestion de ce risque est de diminuer la sévérité ou la probabilité du ou des préjudices afin que le risque puisse être considéré comme proportionné.

N°	Question	Réponse
6)	Quel niveau global de risque est visé ? *[Précisez le niveau global de risque que vous cherchez à atteindre, c'est-à-dire un niveau modéré ou faible si le risque était important ou un niveau faible si le risque était modéré]*	
7)	Pour réaliser cet objectif, le niveau de sévérité à atteindre est de : *[précisez le niveau devant être atteint ou indiquez si celui-ci est d'ores et déjà satisfaisant]*	
8)	Pour réaliser cet objectif, le niveau de probabilité à atteindre est de : *[précisez le niveau devant être atteint ou indiquez si celui-ci est d'ores et déjà satisfaisant]*	

1/ Sévérité du préjudice
[à traiter seulement si le niveau de sévérité doit être réduit]

- Identification des mesures de gestion du risque adaptées

<u>Conséquences du préjudice</u>

N°	Question	Réponse

9)	Existe-t-il des normes techniques applicables au SIA contenant des recommandations relatives aux conséquences du ou des préjudices ?	☐Si oui, indiquez ces recommandations : *Réponse :* ☐Si non, il convient de se reporter à la question 11).
10)	Ces recommandations ont-elles été appliquées ?	☐Si oui, il convient de se reporter à la question 11). ☐Si non, l'application de ces recommandations constitue une mesure de gestion de ce risque.
11)	Paraît-il possible de réduire le niveau des conséquences du ou des préjudices sans porter atteinte à la performance du SIA et à la réalisation de la finalité poursuivie en adoptant d'autres mesures que celles prévues par des normes techniques ?	☐Si oui, les mesures permettant de réduire le niveau des conséquences du ou des préjudices constituent une mesure de gestion de ce risque. ☐Si non, il convient de se reporter à la conclusion.

Conclusion :

Quelles sont les mesures de gestion du risque pouvant être adoptées en réponse à ce problème ?

☐Application de normes techniques. Il convient de mentionner l'application de ces normes dans le Tableau synthétique de l'étude d'impact.

☐Adoption d'autres mesures de gestion du risque pour réduire le niveau des conséquences. Ces mesures doivent être précisées dans le Tableau synthétique de l'étude d'impact.

☐Le niveau des conséquences ne peut pas être réduit sans porter atteinte à la performance du SIA et la réalisation de la finalité poursuivie. Dans ce cas :

☐Il convient de redéfinir la conception du SIA afin de permettre de réduire les conséquences du ou des préjudices (ceci constitue une mesure de gestion de ce risque) ou ;

☐Si cela peut s'avérer suffisant pour atteindre un niveau de risque acceptable, réduire dans une mesure satisfaisante le niveau d'ampleur ou de probabilité du ou des préjudices.

Ampleur du préjudice

N°	Question	Réponse
12)	Existe-t-il des normes techniques applicables au SIA contenant des recommandations relatives à l'ampleur du ou des préjudices ?	☐Si oui, indiquez ces recommandations : *Réponse :* ☐Si non, il convient de se reporter à la question 14).
13)	Ces recommandations ont-elles été appliquées ?	☐Si oui, il convient de se reporter à la question 14). ☐Si non, l'application de ces recommandations constitue une mesure de gestion de ce risque.
14)	Paraît-il possible de réduire le niveau de l'ampleur du ou des préjudices sans porter atteinte à la performance du SIA et à la réalisation de la finalité poursuivie en adoptant d'autres mesures que celles prévues par des normes techniques ?	☐Si oui, les mesures permettant de réduire le niveau de l'ampleur du ou des préjudices constituent une mesure de gestion de ce risque. Il convient d'indiquer plus précisément les mesures pouvant être prises : *Réponse :* ☐Si non, il convient de se reporter à la conclusion.

Conclusion :

Quelles sont les mesures de gestion du risque pouvant être adoptées en réponse à ce problème ?

☐Application de normes techniques. Il convient de mentionner l'application de ces normes dans le Tableau synthétique de l'étude d'impact.

☐Adoption d'autres mesures de gestion du risque pour réduire le niveau de l'ampleur. Ces mesures doivent être précisées dans le Tableau synthétique de l'étude d'impact.

☐Le niveau de l'ampleur ne peut pas être réduit sans porter atteinte au bon fonctionnement du SIA et la réalisation de la finalité poursuivie. Dans ce cas :

☐Il convient de redéfinir la conception du SIA afin de permettre de réduire l'ampleur du ou des préjudices (ceci constitue une mesure de gestion de ce risque) ou ;

☐Si cela peut s'avérer suffisant pour atteindre un niveau de risque acceptable, réduire dans une mesure satisfaisante le niveau de probabilité du ou des préjudices.

Ces mesures de gestion du risque doivent être reportées dans le Tableau synthétique de l'étude d'impact.

2/ Probabilité du préjudice

[à traiter seulement si le niveau de probabilité doit être réduit]

N°	Question	Réponse
15)	Existe-t-il des normes techniques applicables au SIA contenant des recommandations relatives à la probabilité de survenance du ou des préjudices ?	☐Si oui, indiquez ces recommandations : *Réponse :* ☐Si non, il convient de se reporter à la question 17).
16)	Ces recommandations ont-elles été appliquées ?	☐Si oui, il convient de se reporter à la question 17). ☐Si non, l'application de ces recommandations constitue une mesure de gestion de ce risque.
17)	Paraît-il possible de réduire le niveau de probabilité du ou des préjudices sans porter atteinte à la performance du SIA et à la réalisation de la finalité poursuivie en adoptant d'autres mesures que celles prévues par des normes techniques ?	☐Si oui, les mesures permettant de réduire le niveau de probabilité du ou des préjudices constituent une mesure de gestion de ce risque. Il convient d'indiquer plus précisément les mesures pouvant être prises : *Réponse :* ☐Si non, il convient de se reporter à la conclusion.

Quelles sont les mesures de gestion du risque pouvant être adoptées en réponse à ce problème ?

☐Application de normes techniques. Il convient de mentionner l'application de ces normes dans le Tableau synthétique de l'étude d'impact.

☐Adoption d’autres mesures de gestion du risque pour réduire le niveau de probabilité. Ces mesures doivent être précisées dans le Tableau synthétique de l’étude d’impact.

☐Le niveau de probabilité ne peut pas être réduit sans porter atteinte au bon fonctionnement du SIA et la réalisation de la finalité poursuivie. Dans ce cas :

☐Il convient de redéfinir la conception du SIA afin de permettre de réduire la probabilité du ou des préjudices (ceci constitue une mesure de gestion de ce risque) ou ;

☐Si cela peut s’avérer suffisant pour atteindre un niveau de risque acceptable, réduire dans une mesure satisfaisante le niveau de sévérité du ou des préjudices.

Ces mesures de gestion du risque doivent être reportées dans le Tableau synthétique de l’étude d’impact.

2. Conclusion

Il convient, après avoir reporté l’ensemble des mesures de gestion des risques adoptées dans le Tableau synthétique de l’étude d’impact, de se reporter à la partie « 3. Bilan » de la *Fiche-Risques VUE* et de procéder à l’évaluation des effets des mesures de gestion des risques. Il s’agit d’analyser de nouveau le niveau de risque et la proportionnalité du risque en tenant compte des mesures de gestion des risques.

Annexe 7 : Tableau synthétique de l'étude d'impact

Risque n°	Facteur de risque identifié VUE concernée Préjudice	Niveau de risque	Proportionnalité du SIA	Mesures de gestion du risque adoptées	Bilan
1.					
2.					

Annexe 8 : Exemple d'application : SIA de réidentification

Il ne s'agit que d'un exemple parcellaire. Les réponses ne sont pas nécessairement détaillées. Il convient de détailler les réponses le plus précisément précise.

Tableau descriptif :

Numéro	Explication	Question	Réponse
Personnes impliquées dans le cycle de vie du SIA			
1.	[…]	Quelles sont les personnes impliquées dans le projet et leurs responsabilités ? - Dans la conception ? - Dans la vérification et la validation ? - Dans le déploiement ? - Dans l'exploitation et le suivi ?	
La destination du SIA ou les finalités **[…]**			
2.	[…]	Quelles sont la destination ou les finalités du SIA ?	***Améliorer la sécurité des lieux accueillant un nombre important de personnes.***
3.	[…]	Quelles sont les mauvaises utilisations raisonnablement prévisibles ?	***Utilisation à des fins de discrimination.*** ***Diffusion des images sans consentement des personnes.***
Les fonctions du SIA **[…]**			
4.	[…]	Quelles sont les fonctions du SIA ?	***Identifier une première fois un objet ou une personne grâce à une caméra de surveillance puis, sur la base d'une requête, retrouver cet***

			objet ou cette personne sur une autre caméra de surveillance. ***La réidentification est réalisée grâce à une analyse de ressemblance entre la forme et la couleur des objets ou des personnes (par exemple des caractéristiques physiques comme la tenue vestimentaire ou la corpulence).***
5.	[…]	Est-ce que ces tâches peuvent être réalisées sans recours à un SIA ?	***Ces tâches peuvent être effectuées par une personne.***
6.	[…]	Quels sont les avantages du recours à l'IA ?	***L'IA permet d'effectuer cette tâche avec une plus grande efficacité, notamment lorsque le nombre d'objets et de personnes est important.***
7.	[…]	Qui sont les utilisateurs du SIA ?	***Les utilisateurs sont des agents de sécurité.***
Les objets traités par le SIA **[…]**			
8.	[…]	Quels sont les objets ou les personnes concernés ?	***Il peut s'agir d'une grande variété d'objets (véhicules, valises, etc.). Les personnes concernées sont également très variables, il peut s'agir d'usagers de l'aéroport voire même des salariés.***
Le contexte de déploiement du SIA **[…]**			

9.	[…]	Quelles sont les ressources matérielles nécessaire pour utiliser le SIA ?	***Caméras de vidéosurveillance ayant les caractéristiques techniques suivantes : […].*** ***Autres ressources matérielles : […]***
10.	[…]	Dans quels lieux le SIA est-il utilisé ?	***Il est utilisé dans un aéroport qui est un lieu public accueillant un nombre important de personnes.***
11.	[…]	A quels moments le SIA est-il utilisé ?	***Le SIA est appelé à être utilisé durant les heures de fonctionnement de l'aéroport.***
La description technique du SIA **[…]**			
12.	[…]	Quelles sont les données utilisées pour développer, entraîner, valider et tester le SIA ? Quelle est la source de ces données ?	***Données synthétiques***
13.	[…]	Quelles sont les données d'entrée traitées par le SIA lors de son fonctionnement ? Quelle est la source de ces données ?	***Images d'objets et de personnes.*** ***Données issues des caméras de surveillance.***
14.	[…]	Quelles sont les données produites par le SIA lors de son fonctionnement ?	***Le SIA recherche des ressemblances entre les objets et les personnes repérées par les caméras de surveillance. Il fournit un résultat de ressemblance.***
15.	[…]	Quel est le type d'algorithme utilisé ?	***Apprentissage automatique.***

			Néanmoins, en inférence, le SIA n'apprend plus. L'apprentissage est limité à la phase de développement.
16.	[…]	Pourquoi ce type d'algorithme a-t-il été choisi ?	
17.	[…]	Quel est le niveau d'exactitude du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ?	
18.	[…]	Quel est le niveau de robustesse du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ?	
19.	[…]	Quel est le niveau de résilience du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ?	
20.	[…]	Quel est le niveau de cybersécurité du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation	

		raisonnablement prévisibles ?	
La description scalaire du fonctionnement du SIA **[…]**			
21.	- […]	A quelle échelle géographique le SIA est-il utilisé ?	***A l'échelle de l'aéroport.***
22.	[…]	A quelle échelle temporelle le SIA est-il utilisé ?	***Durée indéterminée.***
23.	[…]	A quelle échelle en termes d'objets le SIA est-il utilisé ?	***Plusieurs milliers de personnes ou d'objets par jour.***

Fiche-Risques VUE :

Risque n°1 : Atteinte à la VUE Liberté

1. Détermination du niveau de risque

A. Description du risque

N°	Question	Réponse
1)	Quel est le facteur de risque que présente le SIA ? *[reporter les mots-clefs de l'Index des risques VUE]*	***Vidéosurveillance***
2)	Quelles sont les valeurs de l'Union européenne potentiellement menacées ? *[se reporter à l'Index des risques VUE]*	***Liberté***
3)	Quels sont le ou les préjudices potentiels ?	***Il y a un risque d'atteinte au droit au respect de la vie privée et à la protection des données à caractère personnel des personnes notamment en cas de fuite des données. Préjudice moral.***

Le facteur de risque, la VUE et le ou les préjudices doivent être mentionnés dans le Tableau synthétique de l'étude d'impact.

B. Niveau du risque

a) Sévérité du préjudice

1/ Conséquences :

N°	Question	Réponse
4)	Quelles sont les victimes potentielles ?	***Usagers de l'aéroport***
5)	Quelles sont la nature et l'importance du ou des préjudices ?	***Préjudice moral portant atteinte à la vie privée des conséquences, pouvant avoir des répercussions modérées.***
6)	Quel effort est nécessaire pour faire cesser ou réparer le ou les préjudices ?	***L'effort peut être important, notamment en cas de diffusion des images sur internet. Il est difficile d'en obtenir la suppression.***
7)	Des dispositifs d'enregistrement conformes à l'article 12 de l'AI Act sont-ils prévus ?	***Oui (à préciser)***

- Niveau des conséquences :

Au regard des caractéristiques des personnes concernées, de la nature et de l'importance des préjudices et de l'effort nécessaire pour faire cesser et réparer le préjudice, le niveau des conséquences peut être évalué à un niveau :

☐Faibles (1) ; ☒Modérées (2) ; ☐Importantes (3).

2/ Ampleur :

N°	Question	Réponse
8)	Quel est le nombre de victimes potentielles ?	***Plusieurs centaines voire milliers de personnes peuvent être concernées.***
9)	Quelle est la criticité du secteur ?	***Aéroport. Secteur critique au sens de la directive NIS (cybersécurité).*** ***Cependant ici la défaillance du SIA n'affecte pas le fonctionnement de l'aéroport.***

- Niveau de l'ampleur :

Au regard du nombre de personnes concernées et de la criticité du secteur, le niveau de l'ampleur peut être évalué à un niveau :

☐Individuelle (1) ; ☒Sectorielle (2) ; ☐Systémique (3).

3/ Evaluation de la sévérité du préjudice :

- Niveau des conséquences : *[reporter le niveau des conséquences]* : ☐Faibles (1) ; ☒Modérées (2) ; ☐Importantes (3).
- Niveau de l'ampleur : *[reporter le niveau de l'ampleur]* : ☐Individuelle (1) ; ☒Sectorielle (2) ; ☐Systémique (3).

Conséquences*Ampleur	Niveau de sévérité
1 ou 2	Faible/1
3 ou 4	Modérée/2
6 ou 9	Importante/3

La combinaison des critères des conséquences et de l'ampleur du ou des préjudices aboutissent à un niveau de sévérité :

☐Faible (1) ; ☒Modéré (2) ; ☐Important (3).

b) <u>Probabilité du préjudice</u>

N°	Question	Réponse
10)	Quel est le niveau d'exactitude du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau d'exactitude est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ? *[se reporter à la ques. 17 du Tableau descriptif]*	***[on suppose qu'il est satisfaisant]***
11)	Quel est le niveau de robustesse du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de robustesse est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il	***[on suppose qu'il est satisfaisant]***

	satisfaisant pour garantir la performance du SIA ? *[se reporter à la ques. 18 du Tableau descriptif]*	
12)	Quel est le niveau de résilience du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de résilience est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ? *[se reporter à la ques. 19 du Tableau descriptif]*	***[on suppose qu'il est satisfaisant]***
13)	Quel est le niveau de cybersécurité du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de cybersécurité est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ? *[se reporter à la ques. 20 du Tableau descriptif]*	***[on suppose qu'il est satisfaisant]*** ***Problème concernant l'usage des appareils personnels agents (utilisation de smartphone pour utiliser les images à l'écran)***
14)	Les jeux de données d'entraînement, de validation et de test font-ils l'objet de pratiques de gouvernance et de gestion des données conformes aux dispositions de l'article 10, §2 de l'AI Act ? *[se reporter à la ques. 12 du Tableau descriptif]*	***[on suppose que oui]***

15)	Les jeux de données d'entraînement, de validation et de test sont-ils pertinents, suffisamment représentatifs et, dans toute la mesure possible, exempts d'erreurs et complets au regard de la destination, conformément aux dispositions de l'article 10, §3 de l'AI Act ? Présentent-ils les propriétés statistiques appropriées, y compris, le cas échéant, en ce qui concerne les personnes ou groupes de personnes à l'égard desquels le SIA est destiné à être utilisé, conformément aux dispositions de l'article 10, §3 de l'AI Act ? *[se reporter à la ques. 12 du Tableau descriptif]*	***[on suppose que oui]***
16)	Les jeux de données d'entraînement, de validation et de test tiennent-ils compte, dans la mesure requise par la destination, des caractéristiques ou éléments propres au cadre géographique, contextuel, comportemental ou fonctionnel spécifique dans lequel le SIA est destiné à être utilisé, conformément aux dispositions de l'article 10, §4 de l'AI Act ? *[se reporter à la ques. 12 du Tableau descriptif]*	***[on suppose que oui]***
17)	Est-il prévu de mentionner dans la notice d'utilisation les informations suivantes, conformément aux dispositions de l'article 13 de l'AI Act :	***[on suppose que oui]***

	- la destination du SIA ; - le niveau d'exactitude, y compris les indicateurs utilisés, de robustesse et de cybersécurité qui a servi de référence pour les tests et la validation du SIA et qui peut être attendu, ainsi que toutes circonstances connues et prévisibles susceptibles d'avoir une incidence sur le niveau attendu d'exactitude, de robustesse et de cybersécurité ; - le cas échéant, la performance du SIA en ce qui concerne des personnes ou groupes de personnes spécifiques à l'égard desquels le système est destiné à être utilisé ; - et les ressources informatiques et matérielles nécessaires, la durée de vie attendue du SIA et toutes les mesures de maintenance et de suivi, y compris leur fréquence, nécessaires pour assurer le bon fonctionnement du SIA, notamment en ce qui concerne les mises à jour logicielles ?	
18)	Quelles sont les mesures de contrôle humain mises en place, conformément aux	***Double validation par des agents de la réidentification.***

	dispositions de l'article 14 de l'AI Act ? De quelle façon permettent-elles de réduire la probabilité de survenance du préjudice ?	

- Niveau de probabilité :

Au regard des caractéristiques techniques du SIA et du respect des exigences essentielles de l'AI Act, le niveau de probabilité peut être évalué à un niveau :

☐Faible (1) ; ☒Modérée (2) ; ☐Importante (3). ***[en raison du risque que les agents de sécurité utilisent leurs propres appareils]***

c) Niveau du risque

- Niveau de sévérité : *[reporter le niveau de sévérité]* : ☐Faible (1) ; ☒Modéré (2) ; ☐Important (3).
- Niveau de probabilité : *[reporter le niveau de probabilité]* : ☐Faible (1) ; ☒ Modérée (2) ; ☐Importante (3).
- Niveau du risque :

		Probabilité		
		1	2	3
Sévérité	1	1	2	3
	2	2	4	6
	3	3	6	9

La combinaison des critères de la sévérité et de la probabilité du ou des préjudices aboutissent à un niveau de risque :

☐Faible (1 ou 2) :

Dans ce cas, il n'est pas nécessaire de prendre des mesures de gestion du risque spécifiques à ce risque et il convient de se reporter directement à la partie « 3. Bilan » et *de mentionner dans le Tableau synthétique que le niveau de risque est faible et acceptable dans la colonne Bilan*.

☒Modéré (3 ou 4) :

Dans ce cas, il convient de se reporter à la partie « 2. Contrôle de la proportionnalité » et *de mentionner dans le Tableau synthétique que le niveau de risque est modéré*.

☐Important (6 ou 9) :

Dans ce cas, le risque est présumé disproportionné. Il convient alors de de se reporter directement à la *Fiche-Gestion risque VUE* et *de mentionner dans le Tableau synthétique que le niveau de risque est important*.

Le niveau de risque doit être mentionné dans le Tableau synthétique de l'étude d'impact.

2. Contrôle de la proportionnalité

A. Critère de la nécessité

N°	Question	Réponse
19)	Quelle est la destination ou la finalité poursuivie ? *[se reporter à la ques. 2 du Tableau descriptif]*	***Sécurité dans un aéroport.***
20)	Le recours aux technologies d'IA offre-t-il des avantages significatifs ? Indiquez précisément pour chaque fonction du SIA la plus-value qu'apporte l'IA *[se reporter aux ques. 5 et 6 du Tableau descriptif]*	*Réponse argumentée :* ☒Pour toutes les fonctions du SIA, le recours aux technologies d'IA offre des avantages significatifs. ☐Pour toutes les fonctions du SIA, e recours aux technologies d'IA n'offre pas d'avantages significatifs.
21)	Les conditions de déploiement du SIA (lieux et plages horaires d'utilisation) sont-elles nécessaires pour la mise en œuvre de la destination ou de la finalité poursuivie ? Justifiez ce caractère nécessaire *[se reporter aux ques. 10 et 11 du Tableau descriptif]* :	*Réponse argumentée :* ***Utilisation dans des lieux accueillant un nombre important de personnes. Limite : utilisation en continue même à des moments où il n'y a pas un nombre important de personnes.*** ☐Les conditions de déploiement du SIA correspondent à ce qui est nécessaire pour atteindre la finalité poursuivie. ☒Les conditions de déploiement du SIA ne correspondent pas à ce qui est nécessaire pour atteindre la finalité poursuivie.
22)	L'échelle d'utilisation du SIA est-elle nécessaire pour la mise en œuvre de la destination ou de la finalité poursuivie ? Justifiez ce caractère nécessaire *[se reporter aux ques. 21 et s. du Tableau descriptif]* :	*Réponse argumentée :* ***Le SIA peut traiter un nombre important de données correspondant à un nombre important de personnes accueillies dans l'aéroport. Utilisation locale dans l'aéroport. Utilisation pour une durée indéterminée correspondant à un accueil continu d'un nombre important de personnes tout au long de l'année.*** ☒L'échelle d'utilisation du SIA correspond à ce qui est nécessaire pour atteindre la finalité poursuivie. ☐L'échelle d'utilisation du SIA ne correspond pas à ce qui est nécessaire pour atteindre la finalité poursuivie.

- Conclusion :

☐La mise en œuvre du SIA est nécessaire.

☒La mise en œuvre du SIA n'est pas nécessaire car :

☐Pour toutes les fonctions du SIA, le recours aux technologies d'IA n'offre pas d'avantages significatifs ;

☒Les conditions de déploiement ne correspondent pas à ce qui est nécessaire pour atteindre la destination ou finalité poursuivie ;

☐L'échelle d'utilisation du SIA ne correspond pas à ce qui est nécessaire pour atteindre la destination ou la finalité poursuivie.

B. Critère de la proportionnalité *stricto sensu*

N°	Question	Réponse
23)	Quelle est la destination ou la finalité poursuivie ? *[se reporter à la ques. 2 du Tableau descriptif]*	***Sécurité dans un aéroport.***
24)	Quelle est la nature des intérêts poursuivis par la destination ou par le déployeur du SIA et lesquels sont-ils ? *[précisez s'il s'agit de droits et principes fondamentaux, et lesquels, ou d'autres intérêts, tel un intérêt commercial par exemple. V. Annexe 2 : Charte des droits fondamentaux de l'Union européenne]*	***Sécurité des personnes et des biens. Correspond à la protection de l'intégrité physique des personnes protégée par l'article 3 de la Charte.***

- Conclusion

Au regard de la nature des intérêts poursuivis par la destination ou le déployeur, le risque paraît :

☒Proportionné car il s'agit d'un intérêt général, la mise en œuvre du SIA est donc proportionnée.

☐Disproportionné car il s'agit d'un intérêt particulier, la mise en œuvre du SIA est donc disproportionnée.

C. Conclusion du contrôle de la proportionnalité

☐La mise en œuvre du SIA est nécessaire ET proportionnée *stricto sensu*. Le risque est donc acceptable et aucune mesure de gestion de ce risque n'est requise. Il convient de se reporter ensuite à la partie « 3. Bilan » et *de mentionner dans le Tableau synthétique que la mise en œuvre du SIA est proportionnée*.

☒La mise en œuvre du SIA n'est pas nécessaire ET proportionnée *stricto sensu*. Le risque est donc inacceptable et il convient de mettre en place des mesures de gestion de ce risque. Il convient pour ce faire de se reporter à la *Fiche-Gestion risque VUE*.

Plus précisément, font défaut le ou les caractères : ☒nécessaire ; ☐ proportionné *stricto sensu*. Il convient *de mentionner dans le Tableau synthétique que la mise en œuvre du SIA est disproportionnée et la source de la disproportion*.

Le caractère proportionné ou disproportionné doit être mentionné dans le Tableau synthétique de l'étude d'impact.

3. Bilan

Trois situations doivent être distinguées :

Niveau de risque	Bilan
Le risque d'atteinte aux VUE est faible	Dans ce cas, le risque est présumé proportionné et acceptable. Il convient de mentionner l'acceptabilité du risque dans le *Tableau synthétique de l'étude d'impact*. Il n'est pas nécessaire de prendre des mesures de gestion de ce risque.
Le risque d'atteinte aux VUE est modéré	Risque proportionné et acceptable : Le contrôle de la proportionnalité a permis de conclure que le niveau de risque est proportionné et donc acceptable. Dans ce cas, il convient de mentionner l'acceptabilité du risque dans le *Tableau synthétique de l'étude d'impact dans la colonne Bilan*. Il n'est pas nécessaire de prendre des mesures de gestion de ce risque.
	Risque disproportionné et inacceptable : Le contrôle de la proportionnalité a permis de conclure que le niveau de risque est disproportionné et donc inacceptable. Dans ce cas, les mesures de gestion de risque adoptées (Fiche-gestion risque VUE) doivent permettre d'éliminer le risque ou de réduire la sévérité ou la probabilité du préjudice ou de corriger les défauts liés à la nécessité et à la proportionnalité. Il convient alors de réaliser le bilan de l'étude d'impact. Le bilan consiste à réévaluer le niveau du risque et la proportionnalité du SIA en tenant compte des mesures de gestion des risques identifiées. Deux situations peuvent se présenter :

	- Si le risque a été éliminé par les mesures de gestion des risques, dans ce cas, il faut considérer que le bilan de l'étude d'impact est positif. Il ne faut pas réévaluer le niveau du risque, puisque ce dernier a été éliminé, ni réévaluer la proportionnalité. - Si le risque n'a pas pu être éliminé, dans ce cas il faut évaluer l'effet des mesures de gestion du risque. A cette fin, il convient de reprendre les points suivants en modifiant les réponses afin de prendre en compte les mesures de gestion du risque : o 1. B. Niveau de risque o 2. Contrôle de la proportionnalité. A cette fin, un tableau est présenté ci-après. A l'issue de cette réévaluation, il faut noter les effets des mesures de gestion des risques et préciser si le risque est devenu ou non acceptable. Il convient de noter le résultat dans la colonne Bilan du *Tableau synthétique de l'étude d'impact*.
Le risque d'atteinte aux VUE est <u>important</u>	Le risque est présumé disproportionné et donc inacceptable. Le contrôle de la proportionnalité a permis de conclure que le niveau de risque est disproportionné et donc inacceptable. Dans ce cas, les mesures de gestion de risque adoptées (Fiche-gestion risque VUE) doivent permettre d'éliminer le risque ou de réduire la sévérité ou la probabilité du préjudice ou de corriger les défauts liés à la nécessité et à la proportionnalité. Il convient alors de réaliser le bilan de l'étude d'impact. Le bilan consiste à réévaluer le niveau du risque et la proportionnalité du SIA en tenant compte des mesures de gestion des risques identifiées. Deux situations peuvent se présenter : - Si le risque a été éliminé par les mesures de gestion des risques, dans ce cas, il faut considérer que le bilan de l'étude d'impact est positif. Il ne faut pas réévaluer le niveau du risque, puisque ce dernier a été éliminé, ni réévaluer la proportionnalité. - Si le risque n'a pas pu être éliminé, dans ce cas il faut évaluer l'effet des mesures de gestion du risque. A cette fin, il convient de reprendre les points suivants en modifiant les réponses afin de prendre en compte les mesures de gestion du risque : o 1. B. Niveau de risque o 2. Contrôle de la proportionnalité. A cette fin, un tableau est présenté ci-après. A l'issue de cette réévaluation, il faut noter les effets des mesures de gestion des risques et préciser si le risque est devenu ou non acceptable. Il convient de noter le résultat dans la colonne Bilan du *Tableau synthétique de l'étude d'impact*.

Le tableau suivant reprend les questions des parties précédentes. Il est possible de ne répondre qu'aux seules questions affectées par les mesures de gestion du risques adoptées.

Question	Réponse
<u>Niveau de risque</u>	
Quels sont le ou les préjudices potentiels ?	
Sévérité du préjudice	
Quelles sont les victimes potentielles ?	
Quelles sont la nature et l'importance du ou des préjudices ?	
Quel effort est nécessaire pour faire cesser ou réparer le ou les préjudices ?	
Des dispositifs d'enregistrement conformes à l'article 12 de l'AI Act sont-ils prévus ?	
Au regard des caractéristiques des personnes concernées, de la nature et de l'importance des préjudices et de l'effort nécessaire pour faire cesser et réparer le préjudice, le niveau des conséquences peut être évalué à un niveau :	☐Faibles (1) ; ☐Modérées (2) ; ☐Importantes (3).
Quel est le nombre de victimes potentielles ?	
Quelle est la criticité du secteur ?	
Au regard du nombre de personnes concernées et de la criticité du secteur, le niveau de l'ampleur peut être évalué à un niveau :	☐Individuelle (1) ; ☐Sectorielle (2) ; ☐Systémique (3).
La combinaison des critères des conséquences et de l'ampleur du ou des préjudices aboutissent à un niveau de sévérité :	☐Faible (1) ; ☐Modéré (2) ; ☐Important (3).
Probabilité du préjudice	

Question	Réponse
Quel est le niveau d'exactitude du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau d'exactitude est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ?	
Quel est le niveau de robustesse du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de robustesse est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ?	
Quel est le niveau de résilience du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de résilience est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ?	
Quel est le niveau de cybersécurité du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise	***Interdiction contractuelle imposée aux agents de ne pas avoir sur eux d'appareils personnels. Interdiction d'utiliser les réseaux sociaux.*** ***Anonymisation des données pour flouter les visages des personnes sans perte de performance***

Question	Réponse
utilisation raisonnablement prévisibles ? Ce niveau de cybersécurité est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ?	
Les jeux de données d'entraînement, de validation et de test font-ils l'objet de pratiques de gouvernance et de gestion des données conformes aux dispositions de l'article 10, §2 de l'AI Act ?	
Les jeux de données d'entraînement, de validation et de test sont-ils pertinents, suffisamment représentatifs et, dans toute la mesure possible, exempts d'erreurs et complets au regard de la destination, conformément aux dispositions de l'article 10, §3 de l'AI Act ? Présentent-ils les propriétés statistiques appropriées, y compris, le cas échéant, en ce qui concerne les personnes ou groupes de personnes à l'égard desquels le SIA est destiné à être utilisé, conformément aux dispositions de l'article 10, §3 de l'AI Act ?	
Les jeux de données d'entraînement, de validation et de test tiennent-ils compte, dans la mesure requise par la destination, des caractéristiques ou éléments propres au cadre géographique, contextuel,	

Question	Réponse
comportemental ou fonctionnel spécifique dans lequel le SIA est destiné à être utilisé, conformément aux dispositions de l'article 10, §4 de l'AI Act ?	
Est-il prévu de mentionner dans la notice d'utilisation les informations suivantes, conformément aux dispositions de l'article 13 de l'AI Act : **- la destination du SIA ;** **- le niveau d'exactitude, y compris les indicateurs utilisés, de robustesse et de cybersécurité qui a servi de référence pour les tests et la validation du SIA et qui peut être attendu, ainsi que toutes circonstances connues et prévisibles susceptibles d'avoir une incidence sur le niveau attendu d'exactitude, de robustesse et de cybersécurité ;** **- le cas échéant, la performance du SIA en ce qui concerne des personnes ou groupes de personnes spécifiques à l'égard desquels le système est destiné à être utilisé ;** **- et les ressources informatiques et matérielles nécessaires, la durée de vie**	

Question	Réponse
attendue du SIA et toutes les mesures de maintenance et de suivi, y compris leur fréquence, nécessaires pour assurer le bon fonctionnement du SIA, notamment en ce qui concerne les mises à jour logicielles ?	
Quelles sont les mesures de contrôle humain mises en place, conformément aux dispositions de l'article 14 de l'AI Act ? De quelle façon permettent-elles de réduire la probabilité de survenance du préjudice ?	
Au regard des caractéristiques techniques du SIA et du respect des exigences essentielles de l'AI Act, le niveau de probabilité peut être évalué à un niveau :	☒Faible (1) ; ☐Modérée (2) ; ☐Importante (3).
Niveau du risque : conclusion	
La combinaison des critères de la sévérité et de la probabilité du ou des préjudices aboutissent à un niveau de risque :	☒Faible (1 ou 2) ; ☐Modéré (3 ou 4) ; ☐Important (6 ou 9).
<u>Contrôle de la proportionnalité</u>	
Critère de la nécessité	
Quelle est la destination ou la finalité poursuivie ?	
Le recours aux technologies d'IA offre-t-il des avantages significatifs ? Indiquez précisément pour chaque fonction du SIA la plus-value qu'apporte l'IA *[se reporter aux ques. 5 et 6 du Tableau descriptif]*	*Réponse argumentée :* ☐Pour toutes les fonctions du SIA, le recours aux technologies d'IA offre des avantages significatifs. ☐Pour toutes les fonctions du SIA, e recours aux technologies d'IA n'offre pas d'avantages significatifs.

Question	Réponse
Les conditions de déploiement du SIA (lieux et plages horaires d'utilisation) sont-elles nécessaires pour la mise en œuvre de la destination ou de la finalité poursuivie ? Justifiez ce caractère nécessaire *[se reporter aux ques. 10 et 11 du Tableau descriptif]* :	*Réponse argumentée :* ***Limitation à des horaires identifiées correspondant à un afflux important de personnes.*** ☒Les conditions de déploiement du SIA correspondent à ce qui est nécessaire pour atteindre la finalité poursuivie. ☐Les conditions de déploiement du SIA ne correspondent pas à ce qui est nécessaire pour atteindre la finalité poursuivie.
L'échelle d'utilisation du SIA est-elle nécessaire pour la mise en œuvre de la destination ou de la finalité poursuivie ? Justifiez ce caractère nécessaire *[se reporter aux ques. 21 et s. du Tableau descriptif]* :	*Réponse argumentée :* ☐L'échelle d'utilisation du SIA correspond à ce qui est nécessaire pour atteindre la finalité poursuivie. ☐L'échelle d'utilisation du SIA ne correspond pas à ce qui est nécessaire pour atteindre la finalité poursuivie.
Critère de la proportionnalité *stricto sensu*	
Quelle est la destination ou la finalité poursuivie ? *[se reporter à la ques. 2 du Tableau descriptif]*	
Quelle est la nature des intérêts poursuivis par la destination ou par le déployeur du SIA et lesquels sont-ils ? *[précisez s'il s'agit de droits et principes fondamentaux, et lesquels, ou d'autres intérêts, tel un intérêt commercial par exemple]*	

- Conclusion de la réévaluation du niveau de risque et de la proportionnalité

A l'issue de cette réévaluation du niveau de risque et de la proportionnalité, le risque paraît :

☒Acceptable ;

☐Inacceptable.

Si le risque demeure inacceptable, il convient de repenser la conception et le développement du SIA puis de réaliser de nouveau une étude d'impact jusqu'à ce que le risque puisse être considéré comme acceptable.

Le résultat final doit être reporté dans la colonne finale du Tableau synthétique de l'étude d'impact.

Risque n°2 : Atteinte à la VUE Egalité

1. Détermination du niveau de risque

A. Description du risque

N°	Question	Réponse
1)	Quel est le facteur de risque que présente le SIA ? *[reporter les mots-clefs de l'Index des risques VUE]*	***Tenue vestimentaire*** ***Corpulence***
2)	Quelles sont les valeurs de l'Union européenne potentiellement menacées ? *[se reporter à l'Index des risques VUE]*	***Egalité***
3)	Quels sont le ou les préjudices potentiels ?	***Préjudice moral lié à une discrimination à l'encontre d'une ou groupe de personnes (traitement différent en fonction de la tenue vestimentaire ou de la corpulence pour des usagers dans une même situation)***

Le facteur de risque, la VUE et le ou les préjudices doivent être mentionnés dans le Tableau synthétique de l'étude d'impact.

B. Niveau du risque

a) Sévérité du préjudice

1/ Conséquences :

N°	Question	Réponse
4)	Quelles sont les victimes potentielles ?	***Usagers de l'aéroport***

5)	Quelles sont la nature et l'importance du ou des préjudices ?	***Préjudice moral lié à une mauvaise identification de la personne par le SIA réidentifiée au regard de sa tenue vestimentaire caractéristique (par ex. port d'un voile; cf. corpulence, tatouage, personne en fauteuil roulant, etc.). Atteinte au principe de non-discrimination***
6)	Quel effort est nécessaire pour faire cesser ou réparer le ou les préjudices ?	***Effort modéré, les conséquences psychologiques pour la personne peuvent être faibles ou modérées mais être réparées rapidement.***
7)	Des dispositifs d'enregistrement conformes à l'article 12 de l'AI Act sont-ils prévus ?	***Oui (à préciser)***

- Niveau des conséquences :

Au regard des caractéristiques des personnes concernées, de la nature et de l'importance des préjudices et de l'effort nécessaire pour faire cesser et réparer le préjudice, le niveau des conséquences peut être évalué à un niveau :

☒Faibles (1) ; ☐Modérées (2) ; ☐Importantes (3).

2/ Ampleur :

N°	Question	Réponse
8)	Quel est le nombre de victimes potentielles ?	***Plusieurs centaines voire milliers de personnes peuvent être concernées.***
9)	Quelle est la criticité du secteur ?	***Aéroport. Secteur critique au sens de la directive NIS (cybersécurité).*** ***Cependant ici la défaillance du SIA n'affecte pas le fonctionnement de l'aéroport.***

- Niveau de l'ampleur :

Au regard du nombre de personnes concernées et de la criticité du secteur, le niveau de l'ampleur peut être évalué à un niveau :

☐Individuelle (1) ; ☒Sectorielle (2) ; ☐Systémique (3).

3/ Evaluation de la sévérité du préjudice :

- Niveau des conséquences : *[reporter le niveau des conséquences]* : ☒Faibles (1) ; ☐Modérées (2) ; ☐Importantes (3).
- Niveau de l'ampleur : *[reporter le niveau de l'ampleur]* : ☐Individuelle (1) ; ☒Sectorielle (2) ; ☐Systémique (3).

Conséquences*Ampleur	Niveau de sévérité
1 ou 2	Faible/1
3 ou 4	Modérée/2
6 ou 9	Importante/3

La combinaison des critères des conséquences et de l'ampleur du ou des préjudices aboutissent à un niveau de sévérité :

☐Faible (1) ; ☒Modéré (2) ; ☐Important (3).

b) <u>Probabilité du préjudice</u>

N°	Question	Réponse
10)	Quel est le niveau d'exactitude du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau d'exactitude est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ? *[se reporter à la ques. 17 du Tableau descriptif]*	***[on suppose qu'il est satisfaisant]***
11)	Quel est le niveau de robustesse du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de robustesse est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ? *[se reporter à la ques. 18 du Tableau descriptif]*	***[on suppose qu'il est satisfaisant]***

12)	Quel est le niveau de résilience du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de résilience est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ? *[se reporter à la ques. 19 du Tableau descriptif]*	***[on suppose qu'il est satisfaisant]***
13)	Quel est le niveau de cybersécurité du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de cybersécurité est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ? *[se reporter à la ques. 20 du Tableau descriptif]*	***[on suppose qu'il est satisfaisant]***
14)	Les jeux de données d'entraînement, de validation et de test font-ils l'objet de pratiques de gouvernance et de gestion des données conformes aux dispositions de l'article 10, §2 de l'AI Act ? *[se reporter à la ques. 12 du Tableau descriptif]*	***[on suppose que oui]***
15)	Les jeux de données d'entraînement, de validation et de test sont-ils pertinents, suffisamment représentatifs et, dans toute la mesure possible,	***[on suppose que oui]***

	exempts d'erreurs et complets au regard de la destination, conformément aux dispositions de l'article 10, §3 de l'AI Act ? Présentent-ils les propriétés statistiques appropriées, y compris, le cas échéant, en ce qui concerne les personnes ou groupes de personnes à l'égard desquels le SIA est destiné à être utilisé, conformément aux dispositions de l'article 10, §3 de l'AI Act ? *[se reporter à la ques. 12 du Tableau descriptif]*	
16)	Les jeux de données d'entraînement, de validation et de test tiennent-ils compte, dans la mesure requise par la destination, des caractéristiques ou éléments propres au cadre géographique, contextuel, comportemental ou fonctionnel spécifique dans lequel le SIA est destiné à être utilisé, conformément aux dispositions de l'article 10, §4 de l'AI Act ? *[se reporter à la ques. 12 du Tableau descriptif]*	***[on suppose que oui]***
17)	Est-il prévu de mentionner dans la notice d'utilisation les informations suivantes, conformément aux dispositions de l'article 13 de l'AI Act : - la destination du SIA ; - le niveau d'exactitude, y compris les indicateurs utilisés, de robustesse et de	***[on suppose que oui]***

	cybersécurité qui a servi de référence pour les tests et la validation du SIA et qui peut être attendu, ainsi que toutes circonstances connues et prévisibles susceptibles d'avoir une incidence sur le niveau attendu d'exactitude, de robustesse et de cybersécurité ; - le cas échéant, la performance du SIA en ce qui concerne des personnes ou groupes de personnes spécifiques à l'égard desquels le système est destiné à être utilisé ; - et les ressources informatiques et matérielles nécessaires, la durée de vie attendue du SIA et toutes les mesures de maintenance et de suivi, y compris leur fréquence, nécessaires pour assurer le bon fonctionnement du SIA, notamment en ce qui concerne les mises à jour logicielles ?	
18)	Quelles sont les mesures de contrôle humain mises en place, conformément aux dispositions de l'article 14 de l'AI Act ? De quelle façon permettent-elles de réduire la probabilité de survenance du préjudice ?	***Double validation par des agents de la réidentification.***

- Niveau de probabilité :

Au regard des caractéristiques techniques du SIA et du respect des exigences essentielles de l'AI Act, le niveau de probabilité peut être évalué à un niveau :

☒Faible (1) ; ☐Modérée (2) ; ☐Importante (3).

c) Niveau du risque

- Niveau de sévérité : *[reporter le niveau de sévérité]* : ☐Faible (1) ; ☒Modéré (2) ; ☐Important (3).
- Niveau de probabilité : *[reporter le niveau de probabilité]* : ☒Faible (1) ; ☐ Modérée (2) ; ☐Importante (3).
- Niveau du risque :

		Probabilité		
		1	2	3
Sévérité	1	1	2	3
	2	2	4	6
	3	3	6	9

La combinaison des critères de la sévérité et de la probabilité du ou des préjudices aboutissent à un niveau de risque :

☒Faible (1 ou 2) :

Dans ce cas, il n'est pas nécessaire de prendre des mesures de gestion du risque spécifiques à ce risque et il convient de se reporter directement à la partie « 3. Bilan » et *de mentionner dans le Tableau synthétique que le niveau de risque est faible et acceptable dans la colonne Bilan*.

☐Modéré (3 ou 4) :

Dans ce cas, il convient de se reporter à la partie « 2. Contrôle de la proportionnalité » et *de mentionner dans le Tableau synthétique que le niveau de risque est modéré*.

☐Important (6 ou 9) :

Dans ce cas, le risque est présumé disproportionné. Il convient alors de de se reporter directement à la *Fiche-Gestion risque VUE* et *de mentionner dans le Tableau synthétique que le niveau de risque est important*.

Le niveau de risque doit être mentionné dans le Tableau synthétique de l'étude d'impact.

2. Contrôle de la proportionnalité

3. Bilan

Trois situations doivent être distinguées :

Niveau de risque	Bilan
Le risque d'atteinte aux VUE est <u>faible</u>	Dans ce cas, le risque est présumé proportionné et acceptable. Il convient de mentionner l'acceptabilité du risque dans le *Tableau synthétique de l'étude d'impact*. Il n'est pas nécessaire de prendre des mesures de gestion de ce risque.
Le risque d'atteinte aux VUE est <u>modéré</u>	<u>Risque proportionné et acceptable :</u> Le contrôle de la proportionnalité a permis de conclure que le niveau de risque est proportionné et donc acceptable. Dans ce cas, il convient de mentionner l'acceptabilité du risque dans le *Tableau synthétique de l'étude d'impact dans la colonne Bilan*. Il n'est pas nécessaire de prendre des mesures de gestion de ce risque.
	<u>Risque disproportionné et inacceptable :</u> Le contrôle de la proportionnalité a permis de conclure que le niveau de risque est disproportionné et donc inacceptable. Dans ce cas, les mesures de gestion de risque adoptées (Fiche-gestion risque VUE) doivent permettre d'éliminer le risque ou de réduire la sévérité ou la probabilité du préjudice ou de corriger les défauts liés à la nécessité et à la proportionnalité. Il convient alors de réaliser le bilan de l'étude d'impact. Le bilan consiste à réévaluer le niveau du risque et la proportionnalité du SIA en tenant compte des mesures de gestion des risques identifiées. Deux situations peuvent se présenter : - Si le risque a été éliminé par les mesures de gestion des risques, dans ce cas, il faut considérer que le bilan de l'étude d'impact est positif. Il ne faut pas réévaluer le niveau du risque, puisque ce dernier a été éliminé, ni réévaluer la proportionnalité. - Si le risque n'a pas pu être éliminé, dans ce cas il faut évaluer l'effet des mesures de gestion du risque. A cette fin, il convient de reprendre les points suivants en modifiant les réponses afin de prendre en compte les mesures de gestion du risque : o 1. B. Niveau de risque o 2. Contrôle de la proportionnalité. A cette fin, un tableau est présenté ci-après. A l'issue de cette réévaluation, il faut noter les effets des mesures de gestion des risques et préciser si le risque est devenu ou non acceptable. Il convient de noter le résultat dans la colonne Bilan du *Tableau synthétique de l'étude d'impact*.
Le risque d'atteinte aux	Le risque est présumé disproportionné et donc inacceptable. Le contrôle de la proportionnalité a permis de conclure que le niveau de risque est disproportionné et donc inacceptable. Dans ce cas, les mesures

VUE est <u>important</u>	de gestion de risque adoptées (Fiche-gestion risque VUE) doivent permettre d'éliminer le risque ou de réduire la sévérité ou la probabilité du préjudice ou de corriger les défauts liés à la nécessité et à la proportionnalité. Il convient alors de réaliser le bilan de l'étude d'impact. Le bilan consiste à réévaluer le niveau du risque et la proportionnalité du SIA en tenant compte des mesures de gestion des risques identifiées. Deux situations peuvent se présenter : - Si le risque a été éliminé par les mesures de gestion des risques, dans ce cas, il faut considérer que le bilan de l'étude d'impact est positif. Il ne faut pas réévaluer le niveau du risque, puisque ce dernier a été éliminé, ni réévaluer la proportionnalité. - Si le risque n'a pas pu être éliminé, dans ce cas il faut évaluer l'effet des mesures de gestion du risque. A cette fin, il convient de reprendre les points suivants en modifiant les réponses afin de prendre en compte les mesures de gestion du risque : o 1. B. Niveau de risque o 2. Contrôle de la proportionnalité. A cette fin, un tableau est présenté ci-après. A l'issue de cette réévaluation, il faut noter les effets des mesures de gestion des risques et préciser si le risque est devenu ou non acceptable. Il convient de noter le résultat dans la colonne Bilan du *Tableau synthétique de l'étude d'impact*.

Le tableau suivant reprend les questions des parties précédentes. Il est possible de ne répondre qu'aux seules questions affectées par les mesures de gestion du risques adoptées.

<u>Fiche-Gestion risques VUE :</u>

<u>Risque n°1 : Atteinte à la VUE Liberté</u>

1. <u>Mesures de gestion du risque</u>

   A. <u>Si la mise en œuvre du SIA n'est pas nécessaire</u>

      a) Si le recours aux technologies d'IA n'offre pas d'avantages significatifs

- Objectif des mesures de gestion du risque

L'objectif des mesures de gestion de ce risque consiste à garantir un recours aux technologies d'IA mélioratif. Ainsi, les mesures de gestion de ce risque vise à limiter l'usage

de l'IA aux fonctions pour lesquelles l'IA présente une efficacité accrue par rapport à la réalisation de ces mêmes actions sans recours à l'IA.

- Identification des mesures de gestion du risque adaptées

N°	Question	Réponse
1)	Les fonctions n'offrant pas d'avantages significatifs peuvent-elles être supprimées sans porter atteinte à la performance du SIA ni nuire à la possibilité pour le SIA d'atteindre la finalité poursuivie ?	☐Si oui, lesquelles ? La suppression de ces fonctions constitue une mesure de gestion de ce risque. *Réponse :* ☐Si non, il convient de reconsidérer la conception et le développement du SIA au regard de la destination et de la finalité poursuivie.

Conclusion :

Quelles sont les mesures de gestion du risque pouvant être adoptées en réponse à ce problème ?

Ces mesures de gestion du risque doivent être reportées dans le Tableau synthétique de l'étude d'impact.

b) Si les conditions de déploiement ne correspondent pas à ce qui est nécessaire pour atteindre la finalité poursuivie

- Objectif des mesures de gestion du risque

L'objectif des mesures de gestion de ce risque est d'accorder les conditions de déploiement du SIA à ce qui est nécessaire pour atteindre la destination ou la finalité poursuivie. Il convient à cette fin de redéfinir les conditions de déploiement du SIA.

- Identification des mesures de gestion du risque adaptées

N°	Question	Réponse
2)	Les conditions de déploiement ont-elles été définies par rapport à la destination ou la finalité poursuivie ?	☒Si oui, il convient de réviser les conditions de déploiement par rapport à la destination ou à la finalité poursuivie. Il convient ensuite de se reporter à la question suivante.

		☐Si non, la révision des conditions de déploiement au regard de la finalité poursuivie constitue une mesure de gestion de ce risque.
3)	Est-il possible modifier les conditions de déploiement du SIA sans porter atteinte à la performance du SIA ou à la possibilité de réaliser la finalité poursuivie ?	☒Si oui, la modification des conditions de déploiement constitue une mesure de gestion des risques. ☐Si non, il convient de reconsidérer la conception et le développement du SIA au regard de la destination ou de la finalité poursuivie.

Conclusion :

Quelles sont les mesures de gestion du risque pouvant être adoptées en réponse à ce problème ?

Limitation de l'utilisation du SIA à des horaires connaissant une forte affluence.

Ces mesures de gestion du risque doivent être reportées dans le Tableau synthétique de l'étude d'impact.

c) Si l'échelle d'utilisation du SIA ne correspond pas à ce qui est nécessaire pour atteindre la destination ou la finalité poursuivie

- Objectif des mesures de gestion du risque

L'objectif des mesures de gestion de ce risque est de limiter l'échelle d'utilisation à une mesure n'outrepassant pas ce qui est nécessaire pour atteindre la destination ou la finalité poursuivie.

- Identification des mesures de gestion du risque adaptées

N°	Question	Réponse
4)	L'échelle d'utilisation a-t-elle été déterminée au regard de la destination ou de la finalité poursuivie ?	☐Si oui, il convient de reconsidérer l'adéquation entre l'échelle d'utilisation et la destination et la finalité poursuivie. Pour ce faire, il faut appliquer un principe de « minimisation » de l'utilisation des SIA, selon le problème que pose le SIA au regard du caractère nécessaire. ☐Si non, la réévaluation de l'échelle d'utilisation par rapport à la destination ou à la finalité poursuivie constitue une mesure de gestion de ce risque.

Conclusion :

Quelles sont les mesures de gestion du risque pouvant être adoptées en réponse à ce problème ?

Ces mesures de gestion du risque doivent être reportées dans le Tableau synthétique de l'étude d'impact.

B. Si la mise en œuvre du SIA n'est pas proportionnée *stricto sensu*

- Objectif des mesures de gestion du risque

L'objectif des mesures de gestion de ce risque est :
- D'éliminer le risque de préjudice portant atteinte aux VUE ; ou
- De diminuer la gravité ou la probabilité du ou des préjudices afin que le risque puisse être considéré comme proportionné.

a) Elimination du risque de préjudice

N°	Question	Réponse
5)	Le risque de préjudice peut-il être éliminé sans porter atteinte à la performance du SIA ou à la réalisation de la finalité poursuivie ?	☐Si oui, les mesures permettant d'éliminer ce risque constituent des mesures de gestion de ce risque. Il convient ensuite de se reporter directement à la partie « 3. Bilan » de la Fiche-Risques VUE. Précisez les mesures pouvant être prises pour éliminer ce risque. ☐Si non, il convient de se reporter à la partie suivante « b) Réduction du risque de préjudice ».

Conclusion :
Quelles sont les mesures de gestion du risque pouvant être adoptées en réponse à ce problème ?

Ces mesures de gestion du risque doivent être reportées dans le Tableau synthétique de l'étude d'impact.

b) Réduction du risque de préjudice

- Objectif des mesures de gestion du risque

L'objectif des mesures de gestion de ce risque est de diminuer la sévérité ou la probabilité du ou des préjudices afin que le risque puisse être considéré comme proportionné.

N°	Question	Réponse

6)	Quel niveau global de risque est visé ? *[Précisez le niveau global de risque que vous cherchez à atteindre, c'est-à-dire un niveau modéré ou faible si le risque était important ou un niveau faible si le risque était modéré]*	***Faible***
7)	Pour réaliser cet objectif, le niveau de sévérité à atteindre est de : *[précisez le niveau devant être atteint ou indiquez si celui-ci est d'ores et déjà satisfaisant]*	***Modéré***
8)	Pour réaliser cet objectif, le niveau de probabilité à atteindre est de : *[précisez le niveau devant être atteint ou indiquez si celui-ci est d'ores et déjà satisfaisant]*	***Faible***

1/ Sévérité du préjudice
[à traiter seulement si le niveau de sévérité doit être réduit]

- Identification des mesures de gestion du risque adaptées

Conséquences du préjudice

N°	Question	Réponse
9)	Existe-t-il des normes techniques applicables au SIA contenant des recommandations relatives aux conséquences du ou des préjudices ?	☐Si oui, indiquez ces recommandations : *Réponse :* ☐Si non, il convient de se reporter à la question 11).
10)	Ces recommandations ont-elles été appliquées ?	☐Si oui, il convient de se reporter à la question 11). ☐Si non, l'application de ces recommandations constitue une mesure de gestion de ce risque.

11)	Paraît-il possible de réduire le niveau des conséquences du ou des préjudices sans porter atteinte à la performance du SIA et à la réalisation de la finalité poursuivie en adoptant d'autres mesures que celles prévues par des normes techniques ?	☐Si oui, les mesures permettant de réduire le niveau des conséquences du ou des préjudices constituent une mesure de gestion de ce risque. ☐Si non, il convient de se reporter à la conclusion.

Conclusion :

Quelles sont les mesures de gestion du risque pouvant être adoptées en réponse à ce problème ?

☐Application de normes techniques. Il convient de mentionner l'application de ces normes dans le Tableau synthétique.

☐Adoption d'autres mesures de gestion du risque pour réduire le niveau des conséquences. Ces mesures doivent être précisées dans le Tableau synthétique.

☐Le niveau des conséquences ne peut pas être réduit sans porter atteinte à la performance du SIA et la réalisation de la finalité poursuivie. Dans ce cas :

☐Il convient de redéfinir la conception du SIA afin de permettre de réduire les conséquences du ou des préjudices (ceci constitue une mesure de gestion de ce risque) ou ;

☐Si cela peut s'avérer suffisant pour atteindre un niveau de risque acceptable, réduire dans une mesure satisfaisante le niveau d'ampleur ou de probabilité du ou des préjudices.

Ampleur du préjudice

N°	Question	Réponse
12)	Existe-t-il des normes techniques applicables au SIA contenant des recommandations relatives à l'ampleur du ou des préjudices ?	☐Si oui, indiquez ces recommandations : *Réponse :* ☐Si non, il convient de se reporter à la question 14).
13)	Ces recommandations ont-elles été appliquées ?	☐Si oui, il convient de se reporter à la question 14). ☐Si non, l'application de ces recommandations constitue une mesure de gestion de ce risque.
14)	Paraît-il possible de réduire le niveau de l'ampleur du ou des préjudices sans porter	☐Si oui, les mesures permettant de réduire le niveau de l'ampleur du ou des préjudices constituent une mesure

	atteinte à la performance du SIA et à la réalisation de la finalité poursuivie en adoptant d'autres mesures que celles prévues par des normes techniques ?	de gestion de ce risque. Il convient d'indiquer plus précisément les mesures pouvant être prises : *Réponse :* ☐Si non, il convient de se reporter à la conclusion.

Conclusion :

Quelles sont les mesures de gestion du risque pouvant être adoptées en réponse à ce problème ?

☐Application de normes techniques. Il convient de mentionner l'application de ces normes dans le Tableau synthétique.

☐Adoption d'autres mesures de gestion du risque pour réduire le niveau de l'ampleur. Ces mesures doivent être précisées dans le Tableau synthétique.

☐Le niveau de l'ampleur ne peut pas être réduit sans porter atteinte au bon fonctionnement du SIA et la réalisation de la finalité poursuivie. Dans ce cas :

☐Il convient de redéfinir la conception du SIA afin de permettre de réduire l'ampleur du ou des préjudices (ceci constitue une mesure de gestion de ce risque) ou ;

☐Si cela peut s'avérer suffisant pour atteindre un niveau de risque acceptable, réduire dans une mesure satisfaisante le niveau de probabilité du ou des préjudices.

Ces mesures de gestion du risque doivent être reportées dans le Tableau synthétique de l'étude d'impact.

2/ Probabilité du préjudice

[à traiter seulement si le niveau de probabilité doit être réduit]

N°	Question	Réponse
15)	Existe-t-il des normes techniques applicables au SIA contenant des recommandations relatives à la probabilité de survenance du ou des préjudices ?	☐Si oui, indiquez ces recommandations : *Réponse :* ☒Si non, il convient de se reporter à la question 17).
16)	Ces recommandations ont-elles été appliquées ?	☐Si oui, il convient de se reporter à la question 17). ☒Si non, l'application de ces recommandations constitue une mesure de gestion de ce risque.
17)	Paraît-il possible de réduire le niveau de probabilité du ou des préjudices sans porter	☒Si oui, les mesures permettant de réduire le niveau de probabilité du ou des préjudices constituent une mesure

	atteinte à la performance du SIA et à la réalisation de la finalité poursuivie en adoptant d'autres mesures que celles prévues par des normes techniques ?	de gestion de ce risque. Il convient d'indiquer plus précisément les mesures pouvant être prises : *Réponse :* ***Il est possible de flouter le visage des personnes. Gestion contractuelle du comportement des agents avec le client.*** ☐Si non, il convient de se reporter à la conclusion.

Quelles sont les mesures de gestion du risque pouvant être adoptées en réponse à ce problème ?

☐Application de normes techniques. Il convient de mentionner l'application de ces normes dans le Tableau synthétique.

☒Adoption d'autres mesures de gestion du risque pour réduire le niveau de probabilité. Ces mesures doivent être précisées dans le Tableau synthétique.

☐Le niveau de probabilité ne peut pas être réduit sans porter atteinte au bon fonctionnement du SIA et la réalisation de la finalité poursuivie. Dans ce cas :

☐Il convient de redéfinir la conception du SIA afin de permettre de réduire la probabilité du ou des préjudices (ceci constitue une mesure de gestion de ce risque) ou ;

☐Si cela peut s'avérer suffisant pour atteindre un niveau de risque acceptable, réduire dans une mesure satisfaisante le niveau de sévérité du ou des préjudices.

Ces mesures de gestion du risque doivent être reportées dans le Tableau synthétique de l'étude d'impact.

3. Conclusion

Il convient, après avoir reporté l'ensemble des mesures de gestion des risques adoptées dans le Tableau synthétique de l'étude d'impact, de se reporter à la partie « 3. Bilan » de la *Fiche-Risques VUE* et de procéder à l'évaluation des effets des mesures de gestion des risques. Il s'agit d'analyser de nouveau le niveau de risque et la proportionnalité du risque en tenant compte des mesures de gestion des risques.

Tableau synthétique de l'étude d'impact :

Risque n°	Facteur de risque identifié VUE concernée Préjudice	Niveau de risque	Proportionnalité du SIA	Mesures de gestion du risque adoptées	Bilan
1.	***Vidéosurveillance Liberté***	***Modéré***	***Non-nécessaire***	***1 Limitation de l'utilisation du***	***Acceptable***

	Il y a un risque d'atteinte au droit au respect de la vie privée et à la protection des données à caractère personnel des personnes notamment en cas de fuite des données. *Préjudice moral.*			*SIA sur certaines plages horaires* *2 Gestion contractuelle du risque représenté par une utilisation abusive des images par les agents de sécurité* *3 Anonymisation des données pour flouter les visages des personnes sans perte de performance*	
2.	*Tenue vestimentaire ;* *Corpulence* *Egalité* *Préjudice moral lié à une discrimination à l'encontre d'une ou groupe de personnes (traitement différent en fonction de la tenue vestimentaire ou de la corpulence pour des usagers dans une même situation)*	*Faible*	*Pas de contrôle de la proportionnalité*		*Acceptable*

Annexe 9 : Exemple d'application, ACAS (Airborne alert and Collision Avoidance System)

Il ne s'agit que d'un exemple parcellaire. Les réponses ne sont pas nécessairement détaillées. Il convient de détailler les réponses le plus précisément précise.

Tableau descriptif :

Numéro	Explication	Question	Réponse
Personnes impliquées dans le cycle de vie du SIA			
1.	[…]	Quelles sont les personnes impliquées dans le projet et leurs responsabilités ? - Dans la conception ? - Dans la vérification et la validation ? - Dans le déploiement ? - Dans l'exploitation et le suivi ?	
La destination du SIA ou les finalités **[…]**			
2.	[…]	Quelles sont la destination ou les finalités du SIA ?	***Renforcer l'efficacité des procédures de détection et d'évitement afin de renforcer la sécurité aérienne.***
3.	[…]	Quelles sont les mauvaises utilisations raisonnablement prévisibles ?	
Les fonctions du SIA **[…]**			
4.	[…]	Quelles sont les fonctions du SIA ?	***Le SIA va travailler de manière autonome à partir d'une certaine distance entre les avions. Avant cela, les***

			métriques de l'avion + le contrôle aérien + les pilotes eux-mêmes assurent un contrôle humain pour anticiper toute collision. Après cela, si aucune de ces anticipations n'a été suffisante, ACAS alertera le pilote de manière visuelle et sonore. Si encore une fois, ces alarmes n'engendrent pas de réaction du pilote, alors des manœuvres d'évitement automatiques, seront mises en œuvre par ACAS qui enverra une requête/ commande directement au système de pilotage automatique de l'aéronef.
5.	[…]	Est-ce que ces tâches peuvent être réalisées sans recours à un SIA ?	***Ces tâches sont déjà effectuées par le contrôle au sol (gestion du trafic pour éviter les collisions) et par les pilotes, chargé d'effectuer les procédures d'évitement.***
6.	[…]	Quels sont les avantages du recours à l'IA ?	***Améliore la sécurité, permet de prendre le relai en cas de défaillance du pilote.***
7.	[…]	Qui sont les utilisateurs du SIA ?	***L'utilisateur final est le pilote, l'existence du système sera portée à sa connaissance et il sera entrainé à y réagir /***

			l'utiliser / interagir avec ledit SIA
Les objets traités par le SIA **[…]**			
8.	[…]	Quels sont les objets ou les personnes concernés ?	***Les objets concernés par le SIA sont des aéronefs.***
Le contexte de déploiement du SIA **[…]**			
9.	[…]	Quelles sont les ressources matérielles nécessaire pour utiliser le SIA ?	***Aéronefs équipés d'instruments des appareils de mesures suivants : […]*** ***Système embarqué nécessitant l'utilisation des matériels suivants : […]***
10.	[…]	Dans quels lieux le SIA est-il utilisé ?	***Espace aérien***
11.	[…]	A quels moments le SIA est-il utilisé ?	***Pas de contrainte de temporalité, utilisable H24.***
La description technique du SIA **[…]**			
12.	[…]	Quelles sont les données utilisées pour développer, entraîner, valider et tester le SIA ? Quelle est la source de ces données ?	***Ces données sont standardisées et accessibles par tout membre du RTCA en termes d'accès. En termes d'édition, aucun utilisateur ne peut modifier ces données. Elles sont protégées par diverses mesures de sécurité en termes d'intégrité, chiffrement, RBAC, etc.***
13.	[…]	Quelles sont les données d'entrée traitées par le SIA lors de son fonctionnement ?	***Les données traitées seront des grandeurs physiques, des***

		Quelle est la source de ces données ?	***distances, des angles, vitesses, etc.*** ***Elles proviennent des capteurs de l'aéronef équipé.***
14.	[…]	Quelles sont les données produites par le SIA lors de son fonctionnement ?	***Alarmes pilote (visuelle et sonore)*** ***Prédictions de manœuvre (calculées en creux via un delta des mesures en vol de l'avion)***
15.	[…]	Quel est le type d'algorithme utilisé ?	***Machine learning - Réseau de neurones en mode supervisé, (on donne les entrées et la sortie).***
16.	[…]	Pourquoi ce type d'algorithme a-t-il été choisi ?	***Algorithme le plus adapté/optimisé à ce genre de défis techniques***
17.	[…]	Quel est le niveau d'exactitude du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ?	
18.	[…]	Quel est le niveau de robustesse du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ?	
19.	[…]	Quel est le niveau de résilience du SIA dans des conditions	

		normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ?	
20.	[…]	Quel est le niveau de cybersécurité du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ?	
La description scalaire du fonctionnement du SIA **[…]**			
21.	[…]	A quelle échelle géographique le SIA est-il utilisé ?	***Echelle mondiale.***
22.	[…]	A quelle échelle temporelle le SIA est-il utilisé ?	***Durée indéterminée.***
23.	[…]	A quelle échelle en termes d'objets le SIA est-il utilisé ?	***Conditionnel: 5 ou 6 grandeurs techniques en entrée. Croisées pour définir tous les scénarios/combinaisons possibles dans un contexte opérationnel à partir d'une certaine distance entre les avions.*** ***L'ACAS ne fonctionnera pas sans ce déclencheur. Cependant il sera activable sur toute la flotte d'aéronefs une fois ces conditions de déclenchement rencontrées.***

Fiche-Risques VUE :

Risque n°1 : Atteinte à la VUE Dignité humaine

1. Détermination du niveau de risque

A. Description du risque

N°	Question	Réponse
1)	Quel est le facteur de risque que présente le SIA ? *[reporter les mots-clefs de l'Index des risques VUE]*	***Dispositif de sécurité***
2)	Quelles sont les valeurs de l'Union européenne potentiellement menacées ? *[se reporter à l'Index des risques VUE]*	***Dignité humaine***
3)	Quels sont le ou les préjudices potentiels ?	***Préjudice corporel pour les passagers et le personnel de bord (décès) ; préjudice corporel pour des tiers au sol.***

Le facteur de risque, la VUE et le ou les préjudices doivent être mentionnés dans le Tableau synthétique de l'étude d'impact.

B. Niveau du risque

a) Sévérité du préjudice

1/ Conséquences :

N°	Question	Réponse
4)	Quelles sont les victimes potentielles ?	***Passagers et pilotes ; tiers.***
5)	Quelles sont la nature et l'importance du ou des préjudices ?	***Préjudice corporel. Risque de décès ou de blessures graves.***
6)	Quel effort est nécessaire pour faire cesser ou réparer le ou les préjudices ?	***Préjudice irréparable en cas de décès.***

7)	Des dispositifs d'enregistrement conformes à l'article 12 de l'AI Act sont-ils prévus ?	***Oui (à préciser)***

- Niveau des conséquences :

Au regard des caractéristiques des personnes concernées, de la nature et de l'importance des préjudices et de l'effort nécessaire pour faire cesser et réparer le préjudice, le niveau des conséquences peut être évalué à un niveau :

☐Faibles (1) ; ☐Modérées (2) ; ☒Importantes (3).

2/ Ampleur :

N°	Question	Réponse
8)	Quel est le nombre de victimes potentielles ?	***Plusieurs centaines de personnes.***
9)	Quelle est la criticité du secteur ?	***Aviation. Secteur critique au sens de la directive NIS (cybersécurité).***

- Niveau de l'ampleur :

Au regard du nombre de personnes concernées et de la criticité du secteur, le niveau de l'ampleur peut être évalué à un niveau :

☐Individuelle (1) ; ☒Sectorielle (2) ; ☐Systémique (3).

3/ Evaluation de la sévérité du préjudice :

- Niveau des conséquences : *[reporter le niveau des conséquences]* : ☐Faibles (1) ; ☐Modérées (2) ; ☒Importantes (3).
- Niveau de l'ampleur : *[reporter le niveau de l'ampleur]* : ☐Individuelle (1) ; ☒Sectorielle (2) ; ☐Systémique (3).

Conséquences*Ampleur	Niveau de sévérité
1 ou 2	Faible/1
3 ou 4	Modérée/2
6 ou 9	Importante/3

La combinaison des critères des conséquences et de l'ampleur du ou des préjudices aboutissent à un niveau de sévérité :

☐Faible (1) ; ☐Modéré (2) ; ☒Important (3).

b) <u>Probabilité du préjudice</u>

N°	Question	Réponse
10)	Quel est le niveau d'exactitude du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau d'exactitude est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ? *[se reporter à la ques. 17 du Tableau descriptif]*	***[on suppose qu'il est satisfaisant]***
11)	Quel est le niveau de robustesse du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de robustesse est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ? *[se reporter à la ques. 18 du Tableau descriptif]*	***[on suppose qu'il est satisfaisant]***
12)	Quel est le niveau de résilience du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de résilience est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ?	***[on suppose qu'il est satisfaisant]***

	[se reporter à la ques. 19 du Tableau descriptif]	
13)	Quel est le niveau de cybersécurité du SIA dans des conditions normales d'utilisation et dans des conditions de mauvaise utilisation raisonnablement prévisibles ? Ce niveau de cybersécurité est-il conforme à l'état de l'art, tel qu'il ressort notamment de l'application de normes techniques, et est-il satisfaisant pour garantir la performance du SIA ? *[se reporter à la ques. 20 du Tableau descriptif]*	***[on suppose qu'il est satisfaisant]***
14)	Les jeux de données d'entraînement, de validation et de test font-ils l'objet de pratiques de gouvernance et de gestion des données conformes aux dispositions de l'article 10, §2 de l'AI Act ? *[se reporter à la ques. 12 du Tableau descriptif]*	***[on suppose que oui]***
15)	Les jeux de données d'entraînement, de validation et de test sont-ils pertinents, suffisamment représentatifs et, dans toute la mesure possible, exempts d'erreurs et complets au regard de la destination, conformément aux dispositions de l'article 10, §3 de l'AI Act ? Présentent-ils les propriétés statistiques appropriées, y compris, le cas échéant, en ce qui concerne les personnes ou groupes de personnes à l'égard desquels le SIA est destiné à être utilisé, conformément aux	***[on suppose que oui]***

	dispositions de l'article 10, §3 de l'AI Act ? *[se reporter à la ques. 12 du Tableau descriptif]*	
16)	Les jeux de données d'entraînement, de validation et de test tiennent-ils compte, dans la mesure requise par la destination, des caractéristiques ou éléments propres au cadre géographique, contextuel, comportemental ou fonctionnel spécifique dans lequel le SIA est destiné à être utilisé, conformément aux dispositions de l'article 10, §4 de l'AI Act ? *[se reporter à la ques. 12 du Tableau descriptif]*	***[on suppose que oui]***
17)	Est-il prévu de mentionner dans la notice d'utilisation les informations suivantes, conformément aux dispositions de l'article 13 de l'AI Act : - la destination du SIA ; - le niveau d'exactitude, y compris les indicateurs utilisés, de robustesse et de cybersécurité qui a servi de référence pour les tests et la validation du SIA et qui peut être attendu, ainsi que toutes circonstances connues et prévisibles susceptibles d'avoir une incidence sur le niveau attendu d'exactitude, de robustesse et de cybersécurité ;	***[on suppose que oui]***

	- le cas échéant, la performance du SIA en ce qui concerne des personnes ou groupes de personnes spécifiques à l'égard desquels le système est destiné à être utilisé ; - et les ressources informatiques et matérielles nécessaires, la durée de vie attendue du SIA et toutes les mesures de maintenance et de suivi, y compris leur fréquence, nécessaires pour assurer le bon fonctionnement du SIA, notamment en ce qui concerne les mises à jour logicielles ?	
18)	Quelles sont les mesures de contrôle humain mises en place, conformément aux dispositions de l'article 14 de l'AI Act ? De quelle façon permettent-elles de réduire la probabilité de survenance du préjudice ?	***Contrôle humain assuré par des pilotes formés. Ils sont susceptibles d'agir pour éviter un autre aéronef.***

- Niveau de probabilité :

Au regard des caractéristiques techniques du SIA et du respect des exigences essentielles de l'AI Act, le niveau de probabilité peut être évalué à un niveau :

☒Faible (1) ; ☐Modérée (2) ; ☐Importante (3).

c) <u>Niveau du risque</u>

- Niveau de sévérité : *[reporter le niveau de sévérité]* : ☐Faible (1) ; ☐Modéré (2) ; ☒Important (3).
- Niveau de probabilité : *[reporter le niveau de probabilité]* : ☒Faible (1) ; ☐ Modérée (2) ; ☐Importante (3).
- Niveau du risque :

		Probabilité		
		1	2	3
Sévérité	1	1	2	3
	2	2	4	6
	3	3	6	9

La combinaison des critères de la sévérité et de la probabilité du ou des préjudices aboutissent à un niveau de risque :

☐Faible (1 ou 2) :

Dans ce cas, il n'est pas nécessaire de prendre des mesures de gestion du risque spécifiques à ce risque et il convient de se reporter directement à la partie « 3. Bilan » et *de mentionner dans le Tableau synthétique que le niveau de risque est faible et acceptable dans la colonne Bilan*.

☒Modéré (3 ou 4) :

Dans ce cas, il convient de se reporter à la partie « 2. Contrôle de la proportionnalité » et *de mentionner dans le Tableau synthétique que le niveau de risque est modéré*.

☐Important (6 ou 9) :

Dans ce cas, le risque est présumé disproportionné. Il convient alors de de se reporter directement à la *Fiche-Gestion risque VUE* et *de mentionner dans le Tableau synthétique que le niveau de risque est important*.

Le niveau de risque doit être mentionné dans le Tableau synthétique de l'étude d'impact.

2. Contrôle de la proportionnalité

A. Critère de la nécessité

N°	Question	Réponse
19)	Quelle est la destination ou la finalité poursuivie ? *[se reporter à la ques. 2 du Tableau descriptif]*	***Sécurité des passagers et du personnel de bord.***
20)	Le recours aux technologies d'IA offre-t-il des avantages significatifs ? Indiquez précisément pour chaque fonction du SIA la plus-value qu'apporte l'IA *[se*	*Réponse argumentée :* ***Permet de prendre efficacement le relai en cas d'inaction des pilotes.*** ☒Pour toutes les fonctions du SIA, le recours aux technologies d'IA offre des avantages significatifs. ☐Pour toutes les fonctions du SIA, e recours aux technologies d'IA n'offre pas d'avantages significatifs.

	reporter aux ques. 5 et 6 du Tableau descriptif]	
21)	Les conditions de déploiement du SIA (lieux et plages horaires d'utilisation) sont-elles nécessaires pour la mise en œuvre de la destination ou de la finalité poursuivie ? Justifiez ce caractère nécessaire *[se reporter aux ques. 10 et 11 du Tableau descriptif]* :	*Réponse argumentée :* ***Utilisation lors du vol de l'aéronef sous condition.*** ☒Les conditions de déploiement du SIA correspondent à ce qui est nécessaire pour atteindre la finalité poursuivie. ☐Les conditions de déploiement du SIA ne correspondent pas à ce qui est nécessaire pour atteindre la finalité poursuivie.
22)	L'échelle d'utilisation du SIA est-elle nécessaire pour la mise en œuvre de la destination ou de la finalité poursuivie ? Justifiez ce caractère nécessaire *[se reporter aux ques. 21 et s. du Tableau descriptif]* :	*Réponse argumentée :* ☒L'échelle d'utilisation du SIA correspond à ce qui est nécessaire pour atteindre la finalité poursuivie. ☐L'échelle d'utilisation du SIA ne correspond pas à ce qui est nécessaire pour atteindre la finalité poursuivie.

- Conclusion :

☒La mise en œuvre du SIA est nécessaire.

☐La mise en œuvre du SIA n'est pas nécessaire car :

☐Pour toutes les fonctions du SIA, le recours aux technologies d'IA n'offre pas d'avantages significatifs ;

☐Les conditions de déploiement ne correspondent pas à ce qui est nécessaire pour atteindre la destination ou finalité poursuivie ;

☐L'échelle d'utilisation du SIA ne correspond pas à ce qui est nécessaire pour atteindre la destination ou la finalité poursuivie.

B. Critère de la proportionnalité *stricto sensu*

N°	Question	Réponse
23)	Quelle est la destination ou la finalité poursuivie ? *[se reporter à la ques. 2 du Tableau descriptif]*	***Sécurité des passagers et du personnel de bord.***
24)	Quelle est la nature des intérêts poursuivis par la destination ou par le déployeur du SIA et	***Sécurité des personnes et des biens. Correspond à la protection de l'intégrité physique des personnes protégée par l'article 3 de la Charte.***

	lesquels sont-ils ? *[précisez s'il s'agit de droits et principes fondamentaux, et lesquels, ou d'autres intérêts, tel un intérêt commercial par exemple. V. Annexe 2 : Charte des droits fondamentaux de l'Union européenne]*	

- Conclusion

Au regard de la nature des intérêts poursuivis par la destination ou le déployeur, le risque paraît :

☒Proportionné car il s'agit d'un intérêt général, la mise en œuvre du SIA est donc proportionnée.

☐Disproportionné car il s'agit d'un intérêt particulier, la mise en œuvre du SIA est donc disproportionnée.

C. Conclusion du contrôle de la proportionnalité

☒La mise en œuvre du SIA est nécessaire ET proportionnée *stricto sensu*. Le risque est donc acceptable et aucune mesure de gestion de ce risque n'est requise. Il convient de se reporter ensuite à la partie « 3. Bilan » et *de mentionner dans le Tableau synthétique que la mise en œuvre du SIA est proportionnée*.

☐La mise en œuvre du SIA n'est pas nécessaire ET proportionnée *stricto sensu*. Le risque est donc inacceptable et il convient de mettre en place des mesures de gestion de ce risque. Il convient pour ce faire de se reporter à la *Fiche-Gestion risque VUE*.

Plus précisément, font défaut le ou les caractères : ☒nécessaire ; ☐ proportionné *stricto sensu*. Il convient *de mentionner dans le Tableau synthétique que la mise en œuvre du SIA est disproportionnée et la source de la disproportion*.

Le caractère proportionné ou disproportionné doit être mentionné dans le Tableau synthétique de l'étude d'impact.

3. Bilan

Trois situations doivent être distinguées :

Niveau de risque	Bilan

Le risque d'atteinte aux VUE est <u>faible</u>	Dans ce cas, le risque est présumé proportionné et acceptable. Il convient de mentionner l'acceptabilité du risque dans le *Tableau synthétique de l'étude d'impact*. Il n'est pas nécessaire de prendre des mesures de gestion de ce risque.
Le risque d'atteinte aux VUE est <u>modéré</u>	<u>Risque proportionné et acceptable :</u> Le contrôle de la proportionnalité a permis de conclure que le niveau de risque est proportionné et donc acceptable. Dans ce cas, il convient de mentionner l'acceptabilité du risque dans le *Tableau synthétique de l'étude d'impact dans la colonne Bilan*. Il n'est pas nécessaire de prendre des mesures de gestion de ce risque.
	<u>Risque disproportionné et inacceptable :</u> Le contrôle de la proportionnalité a permis de conclure que le niveau de risque est disproportionné et donc inacceptable. Dans ce cas, les mesures de gestion de risque adoptées (Fiche-gestion risque VUE) doivent permettre d'éliminer le risque ou de réduire la sévérité ou la probabilité du préjudice ou de corriger les défauts liés à la nécessité et à la proportionnalité. Il convient alors de réaliser le bilan de l'étude d'impact. Le bilan consiste à réévaluer le niveau du risque et la proportionnalité du SIA en tenant compte des mesures de gestion des risques identifiées. Deux situations peuvent se présenter : - Si le risque a été éliminé par les mesures de gestion des risques, dans ce cas, il faut considérer que le bilan de l'étude d'impact est positif. Il ne faut pas réévaluer le niveau du risque, puisque ce dernier a été éliminé, ni réévaluer la proportionnalité. - Si le risque n'a pas pu être éliminé, dans ce cas il faut évaluer l'effet des mesures de gestion du risque. A cette fin, il convient de reprendre les points suivants en modifiant les réponses afin de prendre en compte les mesures de gestion du risque : o 1. B. Niveau de risque o 2. Contrôle de la proportionnalité. A cette fin, un tableau est présenté ci-après. A l'issue de cette réévaluation, il faut noter les effets des mesures de gestion des risques et préciser si le risque est devenu ou non acceptable. Il convient de noter le résultat dans la colonne Bilan du *Tableau synthétique de l'étude d'impact.*
Le risque d'atteinte aux VUE est <u>important</u>	Le risque est présumé disproportionné et donc inacceptable. Le contrôle de la proportionnalité a permis de conclure que le niveau de risque est disproportionné et donc inacceptable. Dans ce cas, les mesures de gestion de risque adoptées (Fiche-gestion risque VUE) doivent permettre d'éliminer le risque ou de réduire la sévérité ou la probabilité du

	préjudice ou de corriger les défauts liés à la nécessité et à la proportionnalité. Il convient alors de réaliser le bilan de l'étude d'impact. Le bilan consiste à réévaluer le niveau du risque et la proportionnalité du SIA en tenant compte des mesures de gestion des risques identifiées. Deux situations peuvent se présenter : - Si le risque a été éliminé par les mesures de gestion des risques, dans ce cas, il faut considérer que le bilan de l'étude d'impact est positif. Il ne faut pas réévaluer le niveau du risque, puisque ce dernier a été éliminé, ni réévaluer la proportionnalité. - Si le risque n'a pas pu être éliminé, dans ce cas il faut évaluer l'effet des mesures de gestion du risque. A cette fin, il convient de reprendre les points suivants en modifiant les réponses afin de prendre en compte les mesures de gestion du risque : o 1. B. Niveau de risque o 2. Contrôle de la proportionnalité. A cette fin, un tableau est présenté ci-après. A l'issue de cette réévaluation, il faut noter les effets des mesures de gestion des risques et préciser si le risque est devenu ou non acceptable. Il convient de noter le résultat dans la colonne Bilan du *Tableau synthétique de l'étude d'impact*.

Tableau synthétique de l'étude d'impact :

Risque n°	Facteur de risque identifié VUE concernée Préjudice	Niveau de risque	Proportionnalité du SIA	Mesures de gestion du risque adoptées	Bilan
1.	***Dispositif de sécurité Dignité humaine Préjudice corporel pour les passagers et le personnel de bord (décès) ; préjudice***	***Modéré***	***Proportionné***		***Acceptable***

	corporel pour des tiers au sol.				