De la protection des données à la création de valeur en finance: évaluation des données, comptabilité, fusions-acquisitions et gouvernance

Applications concrètes pour les organisations orientées vers les données

Étude conjointe menée par le département « Dispositifs de confiance » de la CNPD Luxembourg, la mission « Analyse économique » de la CNIL et le département « Economic Analysis » de l'ICO.

Automne 2026

CNPD COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

ico.

Publié en octobre 2026.

Étude conjointe menée par le département « Dispositifs de confiance » de la CNPD Luxembourg, la mission Analyse économique » de la CNIL et le département « Economic Analysis » de l'ICO.

***Auteurs: Elena-Cristina GERTH** (chef de service « Dispositifs de confiance », CNPD Luxembourg), **Angeliki LASHAND** (Head of Economic Analysis, ICO), **Aymeric PONTVIANNE** (Chef de mission Analyse économique, CNIL)*

Contributeurs : Edouard BASSARD (Service « Dispositifs de confiance », CNPD Luxembourg), Oscar COMBE (Mission Analyse économique, CNIL), Ben MAHON (Economic Analysis, ICO)

Soutien éditorial : Angelica FERNANDEZ (Service « Guidance », CNPD Luxembourg), Maud LYSSON (Direction des technologies, de l'innovation et de l'IA, CNIL) et Ryan DUCHENE (Service « communication digitale », CNPD Luxembourg)

Remerciements : nous tenons à remercier pour leur soutien Alain HERRMANN (Commissaire, CNPD Luxembourg), Tom REYNOLDS (Director of Economic Analysis, ICO) et Vincent VILLETTE (Secrétaire général, CNIL).

Nous souhaitons également exprimer notre gratitude aux personnes qui ont participé à cette étude au moyen de questionnaires et d'entretiens, notamment aux participants du Data Protection Laboratory (DaProLab), organisé par la CNPD au Luxembourg, lors de sa session du 6 juillet 2026.

Nota bene : Le présent document présente les conclusions de l'étude menée par la CNPD, la CNIL et l'ICO sur l'interaction entre la conformité en matière de protection des données et la création de valeur au sein des organisations orientées vers les données. Il vise à encourager les échanges sur ce sujet avec les acteurs du marché, les universitaires et les autres autorités de régulation. Les bonnes pratiques émergentes et encouragées qui y sont présentées n'ont pas d'effet juridique.

Table des matières

Synthèse **6**

1 Introduction et objectifs **10**

1.2 Contexte et justification de l'étude 10

1.3 Objectifs et questions clés de l'étude 11

1.2.1 Objectifs de l'étude 11

1.2.2 Questions clés 12

2 Cadre analytique **15**

2.1 Approche méthodologique générale et entretiens 15

2.2 Revue de la littérature 16

2.2.1 Évaluation des données 17

2.2.2 Traitement comptable 21

2.2.3 Cybersécurité 24

2.3 Enquêtes quantitatives 25

3 Résultats de l'étude et pratiques clés **27**

3.1 Aspects stratégiques de la protection des données pour les organisations 28

3.1.1 Une perception différenciée de la protection des données selon les acteurs des marchés financiers 28

3.1.2 La protection des données comme facteur financier et stratégique dans un monde fondé sur les données 29

3.1.3 La gouvernance des données comme condition préalable au déploiement de l'IA 37

3.2 Traitement comptable et exposition financière liés aux enjeux de données 39

3.2.1 Points de vue des parties prenantes sur les données et la conformité en matière de protection des données dans les états financiers 39

3.2.2 Les actifs de données et la protection des données dans l'information financière 43

3.3 Incidences de la conformité à la protection des données sur les transactions et sur l'évaluation financière 58

3.3.1 Enseignements tirés des sources publiques et des entretiens 59

3.3.2 Conformité des données et risques dans les notations de crédit 60

3.3.3 Résultats de l'enquête quantitative 62

3.3.4 Aspects transactionnels (fusions et acquisitions) et considérations relatives à la due diligence 66

3.3.5 Aspects d'évaluation financière 71

3.3.6 Intégration des questions de données dans la méthode des flux de trésorerie actualisés 73

4 Bonnes pratiques émergentes 77

5 Conclusion 83

6 Références 85

Annexes : 88

A. Résultats statistiques 88

1. Méthodologie 88

2. Profil des entreprises et modèles d'affaires 88

3. Données et matérialité financière 91

4. Enjeux de cybersécurité 98

5. Pratiques en matière d'IA 101

6. Enquête menée auprès d'entreprises luxembourgeoises 102

B. Exemple pratique : regroupement d'entreprises portant sur une base de données clients (IFRS 3, IAS 38 et IAS 36) 114

C. Parties prenantes consultées 119

Synthèse

Les données constituent un facteur fondamental de l'activité économique, de l'innovation et de la performance des organisations. Alors que les organisations s'appuient de plus en plus sur les données pour éclairer la prise de décision, développer de nouveaux produits et services, gérer les risques et favoriser l'émergence de technologies telles que l'intelligence artificielle, l'enjeu ne porte plus seulement sur la manière dont les données doivent être protégées et gouvernées, mais également sur la manière dont leur valeur peut être reconnue, mesurée et exploitée. Il faut donc **considérer les données comme une source de création de valeur** et en appréhender concrètement les modalités d'exploitation.

Dans ce contexte, la Commission nationale pour la protection des données (CNPD) au Luxembourg, la Commission nationale de l'informatique et des libertés (CNIL) en France et l'Information Commission's Office (ICO) au Royaume-Uni, ont mené conjointement une étude visant à examiner les liens entre la conformité en matière de protection des données, la gouvernance des données et la création de valeur. Bien que cette étude repose principalement sur des éléments recueillis auprès de parties prenantes actives sur les marchés financiers, ses conclusions sont également pertinentes pour les organisations confrontées à des enjeux similaires en matière de gestion et d'utilisation des données dans **l'ensemble de l'économie numérique.**

L'étude a été conçue autour de trois axes complémentaires.

Tout d'abord, l'étude a cherché à déterminer si la conformité en matière de protection des données et, plus largement, les pratiques de gouvernance des données étaient perçues comme de simples exigences réglementaires ou comme **des éléments stratégiques** contribuant à la confiance, à la résilience organisationnelle, à la compétitivité et à la performance à long terme.

Deuxièmement, l'étude a examiné les **conséquences comptables** de la reconnaissance des données en tant qu'«actif économique». Elle a notamment analysé les méthodes d'évaluation existantes, les conditions de comptabilisation des actifs liés aux données au regard des normes comptables applicables, ainsi que la capacité des référentiels d'information financière actuels à refléter la création de valeur dans une économie fondée sur les données.

Troisièmement, l'étude a analysé le rôle de la conformité en matière de protection des données et des enjeux liés aux données **dans les décisions d'investissement**, les opérations de fusions-acquisitions et les processus de due diligence associés. La qualité des données et le niveau de conformité jouent en effet un rôle croissant dans l'évaluation des risques et l'issue des transactions.

Pour répondre à ces questions, l'étude a combiné une revue de la littérature académique, professionnelle et réglementaire, des entretiens avec les parties prenantes et une enquête quantitative menée auprès d'entreprises. Elle a examiné la manière dont les organisations, les émetteurs, les investisseurs, les associations professionnelles du secteur financier, les cabinets d'audit, les agences de notation, les cabinets d'avocats et les sociétés de conseil évaluent les incidences de la conformité à la protection des données et, plus généralement, les opportunités et les risques liés aux données, ainsi que la manière dont ces considérations influencent la prise de décision des organisations et l'information financière.

Les résultats mettent en évidence la convergence, largement documentée, entre la protection des données, la cybersécurité et la gouvernance de l'IA, soulignant la nécessité d'adopter une **approche intégrée** pour gérer les risques et les opportunités liés aux données.

En outre, le principal enseignement de l'étude est la pertinence d'une approche intégrée des enjeux liés aux données en matière de création de valeur pour les organisations. Il s'agit, dans un premier temps, d'identifier et d'évaluer les bénéfices liés au respect des exigences applicables, le rôle des données au sein de l'organisation et leur contribution à la génération de flux de trésorerie futurs, puis de prendre en compte et d'analyser plus précisément les risques liés aux données susceptibles de réduire ces bénéfices, afin de les atténuer. Cette **approche en deux étapes** permet de traduire la réalité complexe de la gestion de la transparence en performance opérationnelle pour les organisations.

Plus précisément, l'étude s'est essentiellement intéressée à la valeur économique des données. Elle s'est appuyée sur une revue de la littérature de plus en plus abondante consacrée à leur évaluation, ainsi que sur l'analyse des méthodes d'évaluation existantes susceptibles d'être utilisées pour estimer la valeur de la conformité et des données personnelles, notamment les approches fondées sur les coûts, les flux futurs et le marché. Les résultats mettent en évidence un écart entre les pratiques actuelles et les méthodes adaptées à l'évaluation des données personnelles en tant qu'actif, ainsi qu'une **prise en compte partielle de l'importance des données** personnelles dans les cadres environnementaux, stratégiques et de gouvernance. Ces limites méthodologiques et de reporting ont suscité un intérêt croissant de la part des organisations qui traitent des données personnelles, des universitaires, des praticiens et des décideurs publics, qui souhaitent comprendre les méthodes existantes permettant de mesurer et de valoriser les données, d'évaluer leur contribution à la valeur de l'organisation et d'examiner les implications financières et comptables de leur reconnaissance en tant qu'actif.

L'étude a en outre examiné les conditions dans lesquelles les

données peuvent être comptabilisées comme un actif dans les référentiels comptables existants. Une attention particulière a été accordée au traitement des données générées en interne et aux critères comptables requis pour leur comptabilisation en tant qu'actifs. L'étude a mis en évidence un constat récurrent dans la littérature et parmi les parties prenantes : bien que les données soient fréquemment décrites comme l'une des ressources les plus précieuses des organisations, seule une partie de leur valeur apparaît dans les états financiers. Cette situation **suscite un débat croissant** sur la capacité des normes comptables existantes, conçues dans un contexte économique différent, à mieux refléter la création de valeur dans les modèles économiques fondés sur les données.

L'étude a également examiné le rôle des enjeux liés aux données, notamment en matière de conformité et de gouvernance, dans les opérations et les processus d'investissement des entreprises. Les résultats montrent que ces enjeux prennent une importance croissante dans les opérations de fusion-acquisition, les due diligence, les évaluations d'investissement et l'analyse des risques des entreprises. La conformité en matière de protection des données, la qualité, l'accessibilité et la sécurité des données sont de plus en plus considérés comme **des facteurs susceptibles d'influencer l'issue des transactions, la résilience des organisations et la création de valeur à long terme.** Dans ce contexte, une évaluation économique appropriée des actifs liés aux données, ainsi que des enjeux de conformité et de gouvernance apparaît essentielle pour comprendre et mettre en évidence la création de valeur, tout en réduisant les incertitudes et les risques.

Enfin, le rapport met en évidence quelques tendances émergentes et **présente plusieurs bonnes pratiques** observées au sein des organisations et auprès des acteurs de marché. Ces pratiques visent à aider les organisations à gérer leurs actifs liés aux données dans le respect des exigences applicables, à mieux se préparer aux opérations et aux processus de due diligence, et à tirer une valeur stratégique des données en s'appuyant sur la conformité en matière de protection des données.

En synthèse, l'étude met en évidence que la valeur de la conformité en matière de protection des données dépasse la seule mise en œuvre opérationnelle. Une protection efficace des données peut contribuer à renforcer la résilience et la confiance au sein des organisations, tout en renforçant la manière dont celles-ci sont évaluées dans le cadre des transactions et des décisions d'investissement, ainsi que la confiance et la perception des consommateurs. Il est désormais **nécessaire de mieux prendre en compte l'importance économique globale des données** dans les pratiques opérationnelles, notamment **en matière d'évaluation, de traitement comptable et de présentation dans les états financiers.**

Fort de ces conclusions et de ces bonnes pratiques émergentes, le rapport vise à aider les organisations à mieux protéger, évaluer et valoriser leurs actifs de données tout au long de leur cycle de vie et à améliorer la transparence dans l'information financière. Cela permettra en retour de valider les attentes des consommateurs quant à la conformité à la protection des données.

1. Introduction et objectifs

1.1 Contexte et justification de l'étude

Les autorités de protection des données ont pour mission de veiller au respect de la législation en matière de protection des données personnelles. Elles doivent également contribuer au bon fonctionnement des marchés, en permettant aux acteurs d'évoluer dans un environnement équitable et concurrentiel, tout en protégeant les droits des personnes à l'égard de leurs données[1]. Dans l'exercice de ces missions, **elles cherchent à réduire l'incertitude pour les organisations régulées et à renforcer la confiance des personnes** dans l'usage de leurs données personnelles. Pour éclairer leur action, elles développent leur connaissance des marchés qu'elles régulent, dialoguent avec les parties prenantes et analysent les bénéfices et les risques associés aux usages actuels et émergents des données personnelles. Elles s'appuient sur ces éléments pour identifier les enjeux de court terme et y répondre, tout en favorisant, à plus long terme, la stabilité et la résilience des marchés, au service de la croissance économique, de la concurrence et de l'innovation.

Contributeur majeur à la création de valeur économique, le secteur financier compte également parmi les secteurs de l'économie qui utilisent le plus de données. Les activités basées sur les données, y compris l'usage de données personnelles, sont au cœur des modèles d'affaire dans le domaine financier. Dès lors, le respect des exigences en matière de protection et de gouvernance des données constitue une composante importante du fonctionnement de ces organisations. De même, les organisations présentes sur les marchés financiers sont déjà familiarisées avec l'importance d'intégrer la confiance, la transparence et une gestion efficace des risques dans leur gouvernance. Il est donc pertinent d'étendre cette réflexion afin de déterminer si les organisations considèrent la protection des données uniquement comme une exigence réglementaire ou si elles y voient **également un levier potentiel de création de valeur.**

Dans ce contexte, **la Commission Nationale pour la Protection des Données (CNPD) au Luxembourg, la Commission Nationale de l'Informatique et des Libertés (CNIL) en France et l'Information Commission's Office (ICO) au Royaume-Uni** ont collaboré afin de mieux comprendre comment la conformité en matière de protection des données est perçue au sein des organisations du secteur financier. L'initiative a consisté à mener une étude exploratoire auprès des parties prenantes et des organisations opérant sur les marchés financiers, afin de déterminer si la conformité et la mise en œuvre de pratiques robustes en matière de gouvernance des données sont considérées comme des actifs stratégiques contribuant à la résilience des organisations, à leur compétitivité et à la création de valeur.

Aux fins de la présente étude, la référence aux « données » englobe l'ensemble des données que les organisations détiennent dans le cadre normal de leurs activités, y compris les données personnelles. Il est fait spécifiquement référence aux « données personnelles », lorsque le propos concerne des pratiques, une législation ou un traitement qui s'appliquent uniquement aux données personnelles.

1.2 Objectifs et questions clés de l'étude

Les régulateurs disposent d'une expérience avérée des bénéfices de la collaboration entre autorités. Le sujet présente un intérêt transversal et, en collaborant, la CNPD, la CNIL et l'ICO ont mutualisé leurs ressources pour recueillir des points de vue divers et informés auprès des acteurs des marchés financiers au Luxembourg, en France et au Royaume-Uni. Ce travail conjoint permet de mieux appréhender ces questions dans les différents marchés et, ainsi, d'avoir une vision plus approfondie des bénéfices que la réglementation peut apporter aux organisations.

1.2.1 Objectifs de l'étude

L'objectif de cette étude est de produire des éclairages permettant aux autorités de régulation de mieux comprendre les implications économiques et stratégiques de la conformité à la protection des données personnelles et des cadres de gouvernance des données sur les marchés financiers. L'étude vise à examiner la manière dont ces dispositifs influencent la performance des organisations, l'évaluation des risques, les décisions d'investissement et de transaction, ainsi que les évaluations financières des entreprises. Elle cherche également à déterminer dans quelle mesure les données personnelles peuvent être comptabilisées, évaluées et reconnues comme un actif dans les états financiers conformément aux référentiels comptables existants.

Bien que l'étude prenne comme point de départ les marchés financiers et les acteurs qui y participent, **ses enseignements dépassent le cadre du secteur des services financiers** et peuvent nourrir la réflexion des autorités de régulation dans différents secteurs. Ils permettent également d'identifier d'autres domaines

1 « données personnelles » désigne toute information relative à une personne physique identifiée ou identifiable (« personne concernée »); une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, en particulier 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 facteurs spécifiques physiques, physiologiques, génétiques, identité mentale, économique, culturelle ou sociale de cette personne physique. Règlement général sur la protection des données 2016, article 4 et Règlement général sur la protection des données 2016 du Royaume-Uni, article 4

dans lesquels des recherches complémentaires seraient utiles. Les résultats et les bonnes pratiques peuvent être examinés dans le contexte réglementaire propre à chaque pays afin de favoriser l'utilisation de données conformément à la réglementation pour créer de la valeur stratégique et opérationnelle, de faciliter l'utilisation de l'IA dans le respect des droits des personnes et d'atténuer les risques liés à la cybersécurité.

Les résultats de cette étude sont partagés dans ce rapport afin de favoriser une production collective de connaissances entre les parties prenantes, les acteurs du marché, le milieu académique et les autorités de régulation. À cette fin, l'étude présente également quelques tendances émergentes en matière d'évaluation et de bonnes pratiques identifiées dans le but de faciliter le partage des connaissances entre les acteurs.

1.2.2 Questions clés

L'étude s'articule autour de trois grandes thématiques, chacune étant déclinée en plusieurs questions qui ont servi de fil conducteur aux entretiens, à l'enquête et à la revue de la littérature.

A. Perceptions et valeur stratégique de la conformité à la protection des données

- Comment la conformité à la protection des données est-elle perçue au sein de l'écosystème financier ?
- Dans quelle mesure les investisseurs, les prêteurs, les agences de notation, les auditeurs et les conseillers en transactions évaluent-ils la gouvernance des données, leur qualité et la conformité lorsqu'ils évaluent la résilience et la performance à long terme des entreprises ?
- Comment les considérations relatives aux données personnelles sont-elles intégrées à la prise de décision dans les organisations ?
- Quelles pratiques permettent aux organisations d'intégrer la conformité à la protection des données dans leurs stratégies de cybersécurité et d'IA ?

B. Le traitement de la conformité en matière de protection des données comme un actif dans les référentiels comptables

- Des dispositifs de gouvernance des données personnelles solides et de bonnes pratiques en matière de vie privée génèrent-ils des avantages économiques mesurables pour les organisations ?
- Quelles méthodes existent pour comptabiliser, mesurer et évaluer les données, y compris les données personnelles, en tant qu'actif de l'entreprise, et dans quelles conditions comptables les actifs liés aux données peuvent-ils être reconnus dans les états financiers ?

C. La valeur de la conformité en matière de protection des données dans les transactions financières

- Comment la protection des données, la cybersécurité et les facteurs liés à la conformité affectent-ils les évaluations d'entreprises, l'évaluation des risques et la performance financière ?
- Comment les considérations de gouvernance des données et liées à la conformité sont-elles intégrées aux transactions et aux processus financiers tels que les fusions-acquisitions, les processus de due diligence et les décisions d'investissement ?

2. Cadre analytique

2.1 Approche méthodologique générale et entretiens

L'étude porte sur le rôle de la conformité en matière de protection des données, des dispositifs de gouvernance des données et des actifs liés aux données au sein des organisations opérant au Luxembourg, en France et au Royaume-Uni, en accordant une attention particulière aux sociétés cotées en bourse et aux organisations qui participent activement aux marchés de capitaux.

Afin de fournir une compréhension complète de la manière dont les considérations relatives aux données sont évaluées en pratique, l'étude inclut également des acteurs qui influencent ou soutiennent les processus d'investissement, d'évaluation et de reporting, tels que les cabinets d'audit, les professionnels de la comptabilité, les spécialistes de l'évaluation, les agences de notation, les cabinets de conseil et les conseils en transaction.

En outre, l'étude tient compte de l'environnement réglementaire et des obligations de reporting dans lesquels ces organisations évoluent. Elle intègre aussi le point de vue des autorités de régulation et des organismes de normalisation concernés afin d'examiner la manière dont la conformité en matière de protection des données, les dispositifs de gouvernance des données, y compris les considérations de cybersécurité, ainsi que la comptabilisation et l'évaluation des actifs liés aux données sont pris en compte dans le reporting des entreprises, les cadres d'évaluation et les pratiques des marchés financiers.

Ce rapport s'appuie ainsi sur la littérature académique, ainsi que sur la collecte de données qualitatives et quantitatives.

Une revue de littérature a été conduite dans un premier temps, afin d'identifier les approches disponibles, le cas échéant, pour quantifier la valeur des données y compris personnelles. Elle s'est concentrée sur des sources solides et fiables : travaux évalués par les pairs, publications d'institutions publiques appliquant les principes de la recherche et de l'analyse publiques – tels que les rapports de régulateurs – ou les publications d'organisations reconnues, accompagnées de leur méthodologie et de leurs hypothèses. Les conclusions de la revue de littérature ont servi à préparer des entretiens. Les cadres

environnementaux, sociaux et de gouvernance (ESG) existants ont été examinés afin de déterminer s'ils comportaient des références spécifiques aux données personnelles. Les référentiels de normes comptables existants ont également été examinés afin d'examiner s'ils comportaient des règles couvrant la quantification et l'évaluation des données personnelles en tant qu'actif dans les comptes des entreprises.

Des entretiens semi-directifs ont été menés de mars à mai 2026 auprès de professionnels et d'experts d'organisations opérant sur les marchés financiers. Douze entretiens ont été réalisés avec des organisations, dont des cabinets de conseil spécialisés en droit, en application de la législation relative à la protection des données et en fusions-acquisitions, ainsi qu'avec des auditeurs, des associations professionnelles du secteur financier, des associations d'investisseurs, des places boursières, des agences de notation et des autorités de marché. Les entretiens se sont déroulés soit en format hybride, en présentiel et à distance, soit intégralement en ligne.

Les réponses recueillies lors des entretiens ont été synthétisées par grandes thématiques, selon les axes retenus dans les questionnaires. L'analyse de ces réponses a ensuite permis de dégager plusieurs enseignements portant notamment sur la quantification de la valeur des données, les autres indicateurs permettant d'évaluer la valeur des données personnelles, le rôle de la conformité en matière de protection des données dans la gouvernance des organisations, la cybersécurité, le traitement des données dans les pratiques comptables, la valeur des données dans les opérations de fusions-acquisitions, la prise en compte de la conformité en matière de protection des données dans les notations des entreprises ainsi que le rôle de la conformité en matière de la protection des données dans le domaine de l'IA.

Le projet a par ailleurs été présenté pour la première fois lors du Symposium sur la protection de la vie privée à Venise, en avril 2026, afin de recueillir les retours des participants. Après la phase qualitative, **des enquêtes statistiques en ligne ont également été menées auprès des délégués à la protection des données (DPO)** en France et au Luxembourg en mai 2026 afin de recueillir des données quantitatives.

Les résultats préliminaires de l'étude ont été partagés lors d'une séance du **Daprolab de la CNPD en juillet 2026,** afin d'inviter des experts à évaluer les résultats et de recueillir des informations supplémentaires. Toutes les organisations sollicitées pour les entretiens ont été invitées à l'événement. Ce rapport présente les conclusions de notre étude, après avoir recueilli, analysé et examiné les réponses, les éléments probants et les données issues des entretiens, et des enquêtes que nous avons menées.

2.2 Revue de la littérature

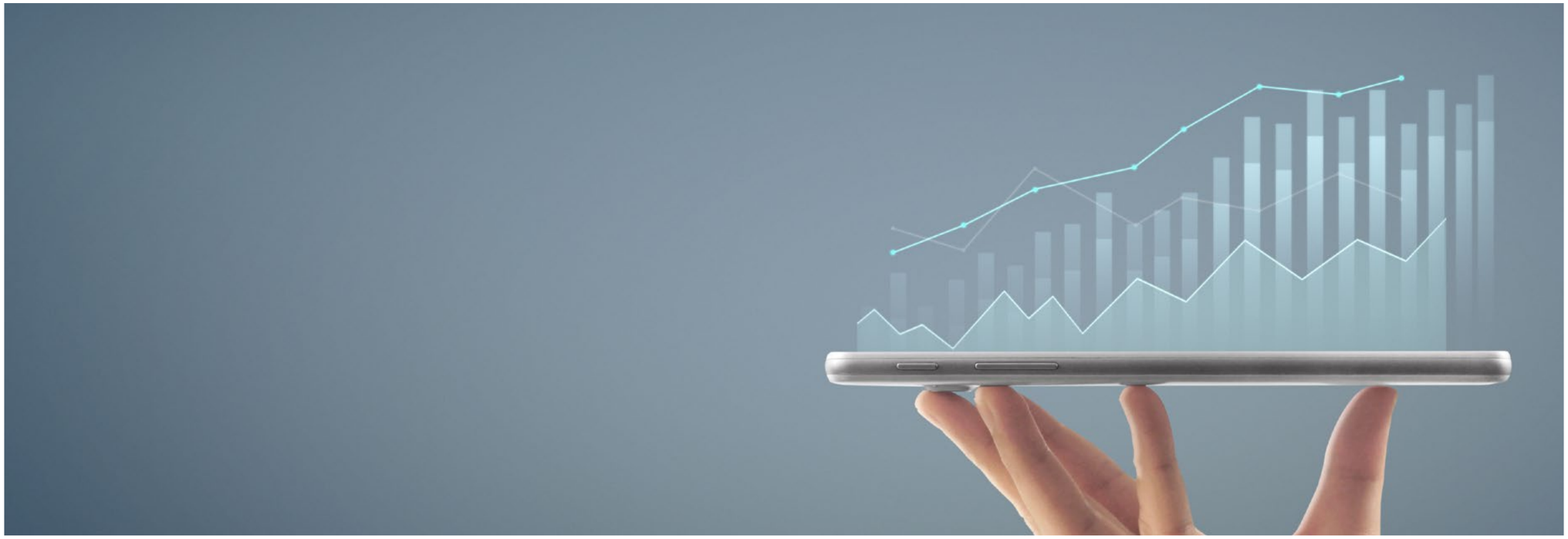
Les résultats de la revue de la littérature portent sur **l'évaluation des données, leur traitement comptable et la cybersécurité.** L'objectif était d'évaluer l'état de l'art des connaissances en matière de prise en compte des données personnelles et des pratiques de gouvernance associées dans le cadre du reporting des entreprises et des processus d'évaluation. La revue de la littérature a en particulier examiné si les cadres comptables existants appréhendaient correctement la valeur des actifs liés aux données, comment les considérations relatives à la protection et à la gouvernance des données affectaient les décisions d'évaluation et d'investissement, et si les facteurs liés à la conformité se traduisaient par des effets financiers mesurables pour les entreprises. Cette revue de la littérature a souvent mis en évidence des éléments relatifs à l'évaluation ou à la comptabilisation des « données », sans distinction entre données et données personnelles. Lorsque la littérature fait référence aux données, nous reprenons également cette terminologie dans notre revue de la littérature ; lorsque la littérature ou nos conclusions font référence aux données personnelles, nous le précisons explicitement.

2.2.1 Évaluation des données

Les données présentent plusieurs caractéristiques propres qui rendent leur évaluation en tant qu'actif délicate. Tout d'abord, les données présentent une importante composante de valeur d'usage. La valeur des données pour une entreprise peut être très différente de celle qu'elle représente pour une autre. L'évaluation d'un même jeu de données peut donc varier d'une organisation à l'autre (Veldkamp, 2023). De plus, les données sont généralement considérées comme non rivales, ce qui signifie qu'elles peuvent être utilisées à plusieurs reprises, y compris par différentes organisations, sans perdre leur valeur. Certaines données perdent néanmoins de la valeur avec le temps, à mesure qu'elles se périment. En outre, les données sont généralement non exclusives, ce qui signifie qu'une fois qu'elles sont disponibles, il est difficile d'empêcher des tiers d'y accéder ou de les utiliser. Cependant, cette caractéristique ne s'applique pas toujours, notamment lorsque les données sont utilisées comme intrants d'un produit ou d'un service et que leur accès peut être restreint par des mécanismes juridiques, techniques ou contractuels. Sur certains marchés, une organisation qui détient des données peut empêcher d'autres organisations de les utiliser. La plupart des données sont des sous-produits d'autres activités économiques, plutôt que des actifs acquis en tant que tels (Veldkamp, 2023). Les organisations peuvent collecter de grands volumes de données à l'occasion d'autres transactions, par exemple via les achats en ligne, ou en proposant des services gratuits tels que des moteurs de recherche ou des réseaux sociaux.

Cela alimente une autre caractéristique essentielle : **les rendements croissants et les économies d'échelle.** L'augmentation de l'activité d'une entreprise génère davantage de données, lesquelles peuvent à leur tour stimuler l'activité, créant ainsi un cercle vertueux. Cela signifie que les données peuvent générer d'importantes économies d'échelle et donc constituer des barrières à l'entrée (OCDE, 2022). Enfin, les données présentent souvent une faible spécificité. Elles peuvent être utilisées à des fins très diverses et réutilisées pour des usages autres que ceux initialement prévus (OCDE, 2022). Une réserve importante, largement absente de la littérature, concerne la distinction entre les données personnelles et les données non personnelles.

Les caractéristiques exposées ci-dessus s'appliquent en grande partie aux données personnelles,



cependant, dans certains cas, celles-ci peuvent faire l'objet d'un accès restreint. Dans ces situations, même si une organisation ne peut pas empêcher une autre de les utiliser, celles qui détiennent d'importants volumes de données personnelles et bénéficient d'effets de réseau peuvent constituer des barrières à l'entrée ou à la croissance pour d'autres organisations détenant les mêmes données. Cela dépend généralement du marché et de la finalité considérés, notamment lorsque quelques acteurs historiques dominent le marché ou lorsque les produits ou services se différencient peu. De même, bien que les organisations puissent utiliser les données personnelles à des fins diverses, ces utilisations doivent rester compatibles avec les droits des personnes concernées sur leurs données, conformément aux garanties prévues par le droit de la protection des données.

Les données créent de la valeur pour les organisations de différentes manières. Veldkamp (2023) soutient que les données bénéficient aux organisations par quatre biais : l'amélioration des processus opérationnels, la réduction des risques, le renforcement du pouvoir de marché et l'innovation. Toutefois, contrairement à la plupart des autres actifs, le principal apport des données réside leur capacité à permettre aux organisations de prendre de meilleures décisions, fondées sur une information plus complète, et à réduire l'incertitude. Cela signifie que les outils de tarification habituellement utilisés en finance pour évaluer les risques jouent un rôle central dans l'évaluation des données. Comme Veldkamp, Farboodi et al. (2025) le constatent, **l'essentiel de la valeur des données financières provient de la réduction des risques.**

Les données constituent une condition préalable essentielle au déploiement de l'IA et à l'entraînement des modèles (Babina, et al., 2024). Elles représentent ainsi un facteur déterminant de la valorisation future de l'entreprise. Deloitte (2025) souligne que des jeux de données ciblés sont indispensables à l'utilisation de l'IA en entreprise. Le cabinet estime également que l'évaluation des données peut aider les conseils d'administration à mieux appréhender l'importance des investissements consacrés aux données. L'évaluation des données pourrait ainsi contribuer à orienter les investissements vers les domaines clés nécessaires à la croissance future. Alors que les conseils d'administration cherchent de plus en plus à déployer l'IA, ces investissements pourraient notamment concerner la collecte, le stockage, le traitement et la mise en conformité des données.

Tambe et al. (2020) quantifient les bénéfices d'un investissement accru dans les données. Plutôt que de se concentrer uniquement sur les données, ils recourent à la notion de capital numérique, qui englobe les données, mais aussi d'autres actifs incorporels, tels que les compétences nécessaires en interne pour traiter et exploiter les données. Ils constatent que, depuis 2010, le capital numérique a augmenté à un rythme environ deux fois supérieur à celui du capital informatique physique. Ils constatent également que l'accumulation de capital numérique est un indicateur significatif de la productivité des entreprises au cours des trois années suivantes. A l'instar de Veldkamp, Xiao et al. (2025) soutiennent **que les données créent de la valeur en réduisant le risque, en permettant aux entreprises de mieux comprendre la demande des consommateurs, en améliorant leurs performances**

et en réduisant les asymétries d'information. Ils montrent également que les actifs liés aux données améliorent sensiblement la qualité des investissements des entreprises. Cet effet est plus marqué dans les grandes entreprises, qui disposent de capacités plus importantes pour investir dans l'analyse et l'exploitation des données.

La littérature distingue généralement **cinq grandes méthodes d'évaluation** (Deloitte, 2025), (Veldkamp, 2023), (OCDE, 2022), (Sargent & Denniston, 2023). La méthode dite des cash flows estime les flux attendus des actifs de données, soit en valeur actuelle, soit en valeur future attendue sur une période donnée. Deloitte (2025) en propose trois déclinaisons. D'abord, la méthode des cash flows sur plusieurs périodes, qui estime directement les flux de trésorerie attribuables aux données et en soustrait les revenus proportionnels attribuables aux autres actifs mobilisés. La méthode prévoit directement les flux attribués aux données, déduit les charges mobilisées pour soutenir les opérations sur les données ou les investissements de conformité, puis actualise les flux nets. Cette méthode est adaptée lorsque la contribution d'un jeu de données à la rentabilité de l'entreprise peut être clairement identifiée.

Deuxièmement, la méthode d'exonération des redevances évalue les données en estimant les redevances que l'entreprise évite de payer parce qu'elle en est propriétaire. Elle est utile lorsque les données permettent clairement d'éviter certains coûts qui auraient été engagés si elles avaient été acquises auprès d'une autre source. Elle est particulièrement pertinente lorsqu'il existe des accords de licence comparables portant sur des sources de données équivalentes. La méthode des flux de trésorerie différentiels compare les cash flow prévisionnels sans l'actif de données à ceux obtenus avec cet actif. Elle compare les performances prévisionnelles de l'entreprise avec et sans l'utilisation des données. La valeur actuelle de cet écart peut être considérée comme la valeur des données. Cette méthode peut être utilisée lorsque le bénéfice généré par les données consiste en un évitement de coûts.

Ensuite, la méthode des coûts consiste à estimer la valeur d'un actif de données en évaluant le coût de sa reproduction ou de son remplacement. Plutôt que de mesurer directement la valeur des données, elle mesure le coût de leur remplacement par un jeu de données équivalent et de qualité comparable. Lorsqu'un jeu de données équivalent est disponible à l'achat, ou peut être facilement constitué, la méthode des coûts peut être facilement utilisée. Cette méthode connaît deux variantes. D'une part, la méthode du coût historique s'appuie sur les coûts passés engagés pour constituer le jeu de données, afin d'estimer les coûts de remplacement. Elle ne tient pas compte des progrès technologiques susceptibles de réduire les coûts, ni du temps écoulé, qui peut rendre impossible la collecte de certaines données historiques. D'autre part, la méthode du coût de reproduction mesure les coûts directs et indirects de création d'un jeu de données, ou estime le prix qu'un prestataire tiers demanderait pour en constituer un équivalent. Bien que la méthode des coûts puisse être simple à utiliser, lorsque le jeu de données est unique et exclusif, il peut être impossible d'en déterminer la valeur selon cette méthode.

La dernière méthode est la méthode par le marché. Elle s'appuie sur les prix payés pour des actifs globalement comparables, en pratique souvent ajustés pour tenir compte de certaines différences entre jeux de données. Le marché des courtiers en données étant assez opaque, les prix des transactions ne sont pas toujours publics et les informations sur les principales caractéristiques des jeux de données nécessaires à leur comparaison font souvent défaut. La rareté des transactions portant sur des jeux de données, et le manque d'information sur celles qui ont lieu, font que cette méthode est rarement utilisée en pratique (Deloitte, 2025). Deloitte la recommande essentiellement comme test de robustesse, en combinaison avec l'approche par les revenus ou par les coûts. A l'inverse, PwC la considère comme la meilleure approche lorsque les transactions sont observables (PwC UK, 2020).

En règle générale, la meilleure pratique consiste à valoriser les données selon deux méthodes distinctes et à rechercher une convergence entre les estimations. Les mêmes grandes approches ont également été appliquées à la comptabilité nationale afin de quantifier la contribution économique des données (OCDE, 2022).

2.2.2 Traitement comptable

Le traitement des données comme un actif en comptabilité s'inscrit dans une réflexion plus large sur l'écart entre ce qui crée de la valeur pour l'entreprise et ce qui est appréhendé dans les états financiers. La littérature met principalement en évidence un décalage à cet égard. Un courant de recherche soutient que la pertinence de la valeur restituée par les états comptables a décliné au fur et à mesure que les actifs incorporels prenaient de l'importance. Lev et Sougiannis (1996) montrent que l'activation de la R&D produit des chiffres plus pertinents pour l'évaluation de la valeur, Lev et Zarowin (1999) documentent une perte d'utilité des états financiers et Lev et Gu (2016) constatent **une corrélation décroissante entre les valeurs de marché et les valeurs comptables** à mesure que les dépenses en actifs incorporels augmentent. Ceci est contesté par Li & McClure (2023), pour qui l'intégration d'éléments relatifs aux actifs incorporels et à des

mesures alternatives de performance n'entraîne pas un déclin de la pertinence combinée pour la valeur, mais révèle plutôt une relation plus complexe.

Les données constituent un actif incorporel présentant des caractéristiques spécifiques. Le rapport de l'ICAEW publié en 2025 souligne la complexité des mécanismes par lesquels les données créent de la valeur, la complexité liée à leur propriété et à leur contrôle juridique, ainsi que la difficulté de les mesurer de manière fiable. Ces éléments correspondent aux critères de comptabilisation prévus par les normes IFRS : l'identifiabilité, le contrôle et la possibilité d'une évaluation fiable. Dans le cadre des IFRS, une entité ne contrôle une ressource que si elle est en mesure d'en diriger l'utilisation et d'en obtenir les avantages. Or, les législations relatives aux données et les règles de protection de la vie privée tendent à limiter le contrôle exercé par l'entreprise sur celles-ci (voir la discussion sur ce point, section 3.2). Estimer la valeur des actifs de données est complexe. L'OCDE (2022) décrit les trois méthodes d'évaluation évoquées précédemment, l'approche par les cash flows, l'approche par les coûts et l'approche par le marché, et conclut qu'aucune ne peut être considérée comme supérieure aux autres. L'objet de ce rapport est de conseiller les bonnes pratiques pour contribuer à surmonter ces limites.

Comme l'explique l'ICAEW, la littérature consacrée à cette question se divise en deux approches. Selon la position plus conservatrice, la comptabilisation des données est difficile en raison des enjeux liés à leur évaluation et à leur propriété. Cette approche privilégie donc des informations plus détaillées dans les notes annexes et les informations qualitatives accompagnant les états financiers (Skinner, 2008) (Wyatt, 2008). L'approche en faveur d'une comptabilisation élargie propose de modifier la norme IAS 38 afin d'admettre davantage d'actifs incorporels générés en interne, la non-comptabilisation étant elle-même susceptible d'éroder la pertinence de l'information (Lev, 2018) (Aboody & Lev, 1998). La révision en cours de la norme IAS 38 par l'IASB est centrale à cet égard.

Cette asymétrie se manifeste également dans le goodwill[2] (écart d'acquisition). Le document de travail de l'EFRAG (2021) souligne qu'un actif incorporel acquis peut être comptabilisé séparément ou inclus dans le goodwill, tandis que ce même actif, lorsqu'il est développé en interne, est passé en charges, ce qui entraîne une distorsion dans les comparaisons entre la croissance externe et la croissance organique. Dans le même sens, Kepler et al. (2026) constatent que les données des consommateurs figurent parmi les actifs incorporels les plus importants comptabilisés lors de l'affectation du prix d'acquisition et que, de ce fait, les données personnelles n'apparaissent aujourd'hui au bilan presque exclusivement qu'à l'occasion d'opérations de fusion-acquisition. En résumé, **la littérature plaide en faveur d'une meilleure comptabilisation des données en tant qu'actif, notamment du point de vue de la transparence et de la fidélité de l'information financière.**

Gao et al. (2025) étudient la manière dont les entreprises intègrent les données dans leurs rapports comptables, à la suite d'une modification réglementaire qui a permis aux entreprises chinoises de comptabiliser les actifs liés aux données dans leurs publications financières. Ils croisent deux enquêtes menées auprès de sociétés cotées avec des données d'archives de 2024 et mettent en évidence un écart important entre valeur perçue des données et les pratiques observées ; seules environ 2 % des entreprises comptabilisaient des actifs liés aux données. Cette situation s'explique par un recul de l'optimisme initial, puis par le fait que les coûts de mise en conformité et les risques de contentieux ont conduit les entreprises à temporiser.

À l'inverse, certaines études se sont intéressées aux bénéfices de la mise en conformité. Un ensemble d'études récentes examine également les conséquences de l'évaluation des données en tant qu'actif. Guo et.al. (2026) évaluent l'incidence des actifs liés aux données sur la valeur des entreprises dans cinq secteurs technologiques, en utilisant des indicateurs comptables (ROA, ROE) et boursiers (Q de Tobin, market-to-book). Ils constatent que l'augmentation de valeur apportée par les actifs de données varie considérablement d'un secteur à l'autre. Wang et Hou (2025) montrent **qu'une meilleure évaluation des données des entreprises en tant qu'actifs réduit significativement les erreurs d'évaluation par le marché, améliorant ainsi l'efficacité globale de l'évaluation du capital.**

2 Le goodwill (écart d'acquisition) est « un actif représentant les avantages économiques futurs résultant des autres actifs acquis dans le cadre d'un regroupement d'entreprises qui ne sont pas identifiés individuellement et comptabilisés séparément » (IFRS 3, Annexe A)

2.2.3 Cybersécurité

Une part importante de la littérature examine l'impact des violations de cybersécurité sur l'évaluation des entreprises. Bien que les incidents de cybersécurité ne constituent pas le seul indicateur de conformité à la protection des données, ils peuvent contribuer à illustrer l'impact d'un faible niveau de conformité à ces obligations sur l'évaluation des entreprises. La conformité peut être difficile à mesurer et à apprécier pour les marchés, mais les incidents de cybersécurité constituent un indicateur de pratiques potentiellement insuffisantes en matière de protection des données et peuvent avoir des effets réputationnels susceptibles d'influencer les décisions des investisseurs et des consommateurs.

Day & Booker (2024) soutiennent que le principal mécanisme par lequel les violations de cybersécurité affectent les évaluations des entreprises passe par la réputation de celles-ci. Ils constatent **des baisses significatives des cours des actions à court terme après une violation.** Ce constat est repris par Martins et al. (2025), qui observent également un impact négatif à court terme des violations de cybersécurité sur un échantillon dans 53 entreprises. Ils constatent par ailleurs des rendements élevés pour les entreprises spécialisées dans la cybersécurité lors de la survenue de violations, ce qui indique que les cyberattaques peuvent entraîner une augmentation des dépenses consacrées aux mesures de protection. L'exposition potentielle à une violation de cybersécurité et les coûts de remédiation qui en découlent pourraient influer sur la perception qu'ont les organisations de l'importance des mesures de protection et du respect des obligations en matière de protection des données.

Les deux articles présentent toutefois des échantillons de petite taille. Muktadir-Al-Mukit & Ali (2025) utilisent un échantillon beaucoup plus important de 776 entreprises et constatent un effet négatif similaire sur les cours de bourse. Les entreprises faisant l'objet **d'attentes sociétales plus élevées en matière de sécurité et de protection la de vie privée,** telles que les entreprises du secteur financier, **subissent un impact plus important** à la suite d'une violation. Ce constat est cohérent avec l'idée selon laquelle la réputation constitue le principal mécanisme par lequel une violation affecte l'évaluation des entreprises. Les auteurs constatent également que la source et la crédibilité des informations relatives à une violation ont eu un impact significatif. Lorsqu'une violation est rapportée par une source jugée « crédible », p. ex. le Financial Times ou CNN, son impact est plus important. Une limite importante réside toutefois dans le biais de sélection observé lorsque les sources « crédibles » sont davantage susceptibles de rendre compte des violations les plus importantes et les plus lourdes de conséquences. Cela pourrait néanmoins souligner l'importance d'une information crédible sur la conformité dans les décisions d'évaluation.

Les violations de cybersécurité peuvent fournir des indications sur les effets à court terme des manquements en matière de protection des données sur les évaluations des entreprises. Il existe également une littérature consacrée à l'étude des évaluations. Cependant, l'impact spécifique du respect des obligations en matière de protection des données, et plus particulièrement du respect des règles relatives aux données personnelles, n'a pas été étudié de manière approfondie dans la littérature.

2.3 Enquêtes quantitatives

Dans le cadre de notre étude, des enquêtes quantitatives en ligne ont été menées en mai 2026 auprès de DPO de France et du Luxembourg, sur la base d'un questionnaire de 25 questions couvrant les modèles d'affaire, la gouvernance, les indicateurs internes, le traitement comptable, les fusions-acquisitions, la cybersécurité et l'IA. L'enquête n'a pas été conduite au Royaume-Uni en raison de contraintes de temps.

En France, l'enquête a porté sur les DPO d'entreprises du secteur privé réalisant plus de 5 millions d'euros de chiffre d'affaires. Elle a recueilli **204 réponses d'entreprises de différents secteurs et de tailles variés,** représentant non seulement le secteur financier, mais également un large éventail d'émetteurs d'instruments financiers, y compris des PME, ce qui a permis de couvrir une grande variété de situations avec une bonne représentativité statistique.

Les DPO ont été invités à remplir le questionnaire avec l'aide de la direction financière de leur entreprise, afin de recuillir les connaissances pertinentes en matière de pratiques comptables et d'évaluation. Les résultats sont présentés à l'annexe A. Les effets étudiés sont statistiquement significatifs, ce qui témoigne de la qualité de la base de données constituée. Au-delà de la pertinence des thématiques abordées, l'objectif de l'enquête était de créer des passerelles entre les équipes DPO, dont l'expertise porte principalement sur les aspects juridiques et informatiques, et les équipes financières. D'après les retours recueillis, cette démarche s'est révélée fructueuse dans le cadre de l'enquête menée en France.

Au Luxembourg, l'échantillon de l'enquête était composé de DPO d'entreprises sélectionnées dans le registre officiel de la CNPD, en donnant la priorité aux entreprises comptant les effectifs les plus importants. Les résultats de l'analyse statistique menée à partir des pratiques recensées dans le cadre des enquêtes sont présentées à l'annexe A. Pour les deux enquêtes menées en France et au Luxembourg, les résultats sont présentés sous une forme agrégée. Ils reposent, lorsque cela est pertinent, sur des statistiques descriptives, des analyses de corrélation et des régressions logistiques. Les réponses des différentes entreprises individuelles n'ont été ni publiées ni partagées entre les autorités participant au projet.

La CNIL, la CNPD et l'ICO tiennent à **remercier les DPO participants et leurs organisations pour le temps qu'ils ont consacré à cette étude** et pour la qualité de leurs analyses et contributions sur ce sujet émergent.

3. Résultats de l'étude et pratiques clés

Cette section présente les principaux résultats de l'étude ainsi que les pratiques clés identifiées lors d'entretiens menés auprès d'acteurs des marchés financiers et d'autres parties prenantes concernées, complétés par les résultats quantitatifs d'une enquête et par une analyse qualitative.

L'analyse est structurée autour de **trois thèmes interdépendants** qui ressortent des résultats de l'analyse qualitative et quantitative. Tout d'abord, elle examine la **perception de la conformité** en matière de protection des données comme un actif stratégique pour les organisations. Elle analyse notamment l'impact différencié de la protection des données selon les acteurs des marchés financiers, son importance stratégique croissante, ainsi que le rôle de la gouvernance des données comme condition préalable au déploiement de l'IA.

Deuxièmement, elle **étudie les implications comptables** des données et des questions liées à la protection des données, en particulier leur représentation dans l'information financière, le traitement comptable des actifs de données, ainsi que la comptabilisation, l'évaluation et la dépréciation des bases de données au regard des normes comptables existantes[3]. Troisièmement, elle analyse les **implications de la conformité** en matière de protection des données sur les transactions et les évaluations financières, notamment son influence sur la valeur des données clients, les évaluations de crédit, les opérations de fusion-acquisition, les due diligence relative aux données et sur l'évaluation des actifs de données.

Dans leur ensemble, ces résultats montrent que la protection des données ne se limite plus à une obligation de conformité, mais constitue désormais un enjeu stratégique, financier et d'investissement dans une économie fondée sur les données.

3 Le principe fondamental de la norme comptable internationale IAS 36 est qu'un actif ne doit pas être inscrit au bilan à une valeur supérieure au montant le plus élevé pouvant être recouvré par son utilisation ou sa cession. Si la valeur comptable dépasse la valeur recouvrable, l'actif est considéré comme ayant subi une perte de valeur - IAS 36 Dépréciation des actifs.

3.1 Aspects stratégiques de la protection des données pour les organisations

3.1.1 Une perception différenciée de la protection des données selon les acteurs des marchés financiers

Les résultats indiquent que l'importance accordée à la protection des données varie selon les acteurs des marchés financiers. Sa valeur perçue, les risques qui lui sont associés et sa pertinence stratégique varient plutôt en fonction des parties prenantes, de leurs responsabilités réglementaires et de leurs objectifs en matière de prise de décision. Tout au long des entretiens, les participants ont systématiquement souligné que la protection des données a dépassé le cadre d'une simple exigence de conformité et qu'elle est de plus en plus intégrée à des considérations plus larges liées à la gouvernance, à la gestion des risques, à la résilience opérationnelle et à la création de valeur.

Pour les **investisseurs et les établissements financiers,** le niveau de maturité en matière de protection des données est généralement considéré comme un indicateur de la qualité de la gouvernance dans des environnements fortement tributaires des données, y compris personnelles. Les participants aux entretiens ont associé des cadres solides de gouvernance des données à une plus grande fiabilité opérationnelle, à une meilleure gestion des risques et à une résilience accrue des organisations. À l'inverse, des dispositifs de gouvernance des données insuffisamment robustes peuvent être perçus comme une source de risque de perte, en particulier dans les organisations qui traitent d'importants volumes de données personnelles. Dans ce contexte, le principe de protection de la vie privée dès la conception (privacy by design) est appelé à être de plus en plus intégré aux processus opérationnels et décisionnels, reflétant l'importance croissante de la gouvernance des données dans les évaluations des investissements et des risques.

Les auditeurs, les consultants et les conseils juridiques ont indiqué que les évaluations portaient généralement sur l'existence d'inventaires des données personnelles ainsi que sur la licéité des traitements. Les lacunes identifiées au cours de ces examens peuvent avoir une incidence sur le calendrier des transactions, augmenter les coûts de mise en conformité ou influencer les évaluations. Ces résultats suggèrent que les enjeux liés à la protection des données sont de plus en plus intégrés aux analyses financières, juridiques et transactionnelles.

Pour les **agences de notation,** la protection des données est principalement prise en compte dans le cadre d'évaluations plus larges de la cybersécurité, de la résilience opérationnelle et de la gestion des risques de l'entreprise. Les participants ont expliqué que les analyses intégraient fréquemment des indicateurs tels que les violations de données, les incidents liés aux rançongiciels et d'autres événements liés à la cybersécurité. Dans ce contexte, le niveau de maturité des dispositifs de gouvernance des données est jugé pertinent lorsqu'il peut avoir une incidence sur la performance opérationnelle, la résilience ou le profil financier à long terme d'une organisation.

Les participants aux entretiens ont noté que l'expérience tirée des violations de données et des incidents de cybersécurité passés avait conduit de nombreuses organisations à renforcer leurs dispositifs de gouvernance des données et de gestion des risques. Dans plusieurs cas, ces événements ont conduit à une surveillance accrue des risques liés aux données par la direction et le conseil d'administration, traduisant une prise de conscience croissante des conséquences financières, opérationnelles et réputationnelles des défaillances en matière de protection des données. Cette prise de conscience demeure toutefois inégale au sein des organisations des marchés financiers, les incidents de cybersécurité constituant un facteur déclencheur pour porter les enjeux liés à la protection et à la gouvernance des données à l'attention des conseils d'administration.

Dans l'ensemble, les résultats montrent que les acteurs des marchés financiers appréhendent la protection des données à travers des angles différents mais interdépendants. Les investisseurs tendent à mettre l'accent sur la qualité de la gouvernance et la gestion des risques, les auditeurs se concentrent sur la conformité et la préparation aux transactions, tandis que les agences de notation évaluent les implications en matière de résilience opérationnelle et de solvabilité. Ensemble, ces perspectives illustrent la manière dont la protection des données s'est progressivement intégrée au secteur financier, non seulement par l'intermédiaire des cadres réglementaires, mais aussi à travers les décisions d'investissement, les processus de due diligence, les transactions de portefeuille, les notations d'entreprise et la gouvernance de la cybersécurité.

Au-delà de la conformité, une gouvernance efficace des données contribue à instaurer la confiance, favorise l'utilisation et la réutilisation des données et permet aux organisations de prendre des décisions mieux éclairées.

3.1.2 La protection des données comme facteur financier et stratégique dans un monde fondé sur les données

La valeur de la conformité à la protection des données pour les organisations

Les données personnelles constituent une ressource essentielle pour de nombreuses organisations, leur permettant de proposer leurs produits et services. Elles sont largement reconnues comme **une source de création de valeur dans des secteurs fortement tributaires des données, tels que la technologie, les plateformes numériques, les services financiers, l'assurance, la santé et le commerce électronique.** Dans le secteur bancaire, par exemple, la collecte de données permet aux organisations de se conformer aux réglementations sectorielles, notamment aux règles relatives à la lutte contre le blanchiment de capitaux (LCB-FT) et est considérée comme présentant une valeur importante. En outre, l'un des éléments centraux des modèles économiques bancaires réside dans la collecte et l'utilisation des données personnelles. Même dans ces secteurs fortement tributaires des données, les données personnelles ont une valeur théorique et sont rarement comptabilisées comme un actif distinct. Les méthodes d'estimation ainsi que les difficultés liées à l'évaluation des données personnelles en tant qu'actifs ont

été examinées en détail dans la revue de la littérature. Les résultats des entretiens ont complété cette analyse et ont montré que la valeur des données personnelles se reflétait plutôt indirectement dans l'efficacité opérationnelle et les informations qu'elles permettaient d'acquérir sur les clients. Au-delà de la valeur des données personnelles en tant que ressources, **la qualité des données, leur traçabilité et la licéité de leur usage deviennent des atouts opérationnels pour les modèles économiques.** Ce constat rejoint les conclusions de la littérature selon laquelle les données personnelles créent de la valeur en améliorant les processus opérationnels, en réduisant les risques, en renforçant le pouvoir de marché et en stimulant l'innovation (Veldkamp, 2023, Farboodi et al., 2025).

Examinons à présent la valeur de la conformité en matière de protection des données personnelles. Notre étude a montré que le respect de la réglementation relative à la protection des données était de plus en plus considéré comme un actif stratégique qui crée de la valeur pour les organisations du secteur financier. Il s'agit d'un constat important, car les évaluations de la conformité en matière de protection des données personnelles tendent à se concentrer sur les coûts de mise en conformité, ceux-ci étant plus immédiats et plus faciles à quantifier. Ainsi, les conseils d'administration et les décideurs ont traditionnellement considéré la conformité en matière de protection des données comme un simple coût. Par exemple, certains participants aux entretiens ont relevé que, dans le secteur bancaire, la conformité en matière de protection des données était perçue comme une contrainte en raison des coûts qu'elle implique. Notre étude des méthodes d'évaluation financière a mis en évidence deux limites découlant de **l'absence de méthodes d'évaluation financière standardisées, qui peuvent expliquer en partie cette perception de la conformité comme simple coût**. Tout d'abord, malgré sa capacité à faciliter les activités, le rôle de la conformité en matière de protection des données tend à s'effacer en tant que facteur stratégique et elle est moins perçue comme susceptible d'offrir un avantage concurrentiel. Deuxièmement, les méthodes d'évaluation actuelles peuvent sous-estimer les risques liés aux données, en particulier dans les transactions où les données personnelles constituent un actif important. La valeur des bénéfices est souvent appréhendée au moyen d'indicateurs non monétaires, tels que la réduction des risques réglementaires et réputationnels, le renforcement de la confiance des investisseurs, des clients et des partenaires, ainsi que l'amélioration de l'accès aux marchés, aux procédures de passation de marchés et aux financements publics. Par exemple, la conformité au RGPD est une exigence formelle pour accéder aux financements de la recherche de l'Union européenne, des lignes directrices ayant été publiées sur le traitement des données sensibles dans le cadre de recherches financées par l'UE[4]. **Au-delà de la valeur que la conformité en matière de protection des données apporte sur le plan stratégique, elle joue également un rôle important dans les activités courantes des organisations.** Celles-ci comprennent notamment les accords de partage de données, qui constituent des documents transactionnels importants relevant de la responsabilité du conseil d'administration et nécessitant un examen par les délégués à la protection des données (DPO). Parmi les autres exemples figurent les processus de due diligence, les garanties et déclarations contractuelles, ainsi que les évaluations des risques réalisées par les investisseurs.

Certains participants à l'étude ont indiqué que, bien que la conformité à la protection des données ne soit pas nécessairement perçue comme activité créatrice de valeur en soi pour les organisations au-delà de l'obligation réglementaire, la non-conformité représentait en revanche un risque financier quantifiable susceptible d'avoir une incidence négative sur l'évaluation des organisations. Dans ce cas, la valeur de la conformité en matière de protection des données réside dans son rôle de facteur de risque, intégré aux évaluations plus larges de la cybersécurité et de la gouvernance, et constitue une composante de l'exposition aux risques mesurables. Les données non conformes n'ont alors pas de valeur de marché, et **la conformité constitue une condition préalable à la reconnaissance des données en tant qu'actif, plutôt qu'un actif en soi.**

Au cours de l'étude, nous avons également identifié un ensemble d'indicateurs couramment utilisés pour communiquer le niveau de maturité en matière de conformité et de fiabilité d'une organisation auprès des consommateurs, des partenaires commerciaux, des marchés et des investisseurs. Ces indicateurs comprennent les économies de coût réalisées grâce à la réutilisation des dispositifs de contrôle de la conformité, l'éligibilité à des procédures de passation de marchés restreintes, la réduction des primes d'assurance contre les risques cyber, le renforcement de la confiance

4 Ethics and data protection, European Commission, 2018.

et l'augmentation des taux de conversion, ainsi que l'efficacité dans le traitement dans le traitement des demandes des personnes concernées.

Les certifications en matière de protection des données, reconnues dans différents secteurs, sont également considérées comme des mécanismes permettant de créer de la valeur, en fournissant des éléments de preuve indépendants, émanant de tiers, attestant de la conformité. Elles renforcent la crédibilité grâce à une évaluation objective, en bénéficiant d'une reconnaissance réglementaire, et en augmentant la visibilité dans les procédures de passation des marchés publics.

La conformité en matière de protection des données comme composante de la gouvernance organisationnelle

Les résultats de l'étude indiquent que les organisations qui intègrent la protection des données dans leurs cadres plus larges de gouvernance peuvent créer de la valeur à long terme grâce à une amélioration de la qualité des données, à une plus grande efficacité opérationnelle, à un renforcement de la résilience organisationnelle et à une confiance accrue des parties prenantes.

Les participants ont indiqué que l'efficacité opérationnelle dans la collecte, le traitement et le stockage des données à caractère personnel pouvait permettre d'en élargir les usages, contribuant ainsi à augmenter les revenus générés. Nous avons par ailleurs constaté que la protection des données constituait une exigence commune à d'autres cadres réglementaires. Les efforts consentis pour s'y conformer permettent donc aux organisations de satisfaire simultanément à plusieurs obligations réglementaires, de réutiliser des contrôles existants, d'optimiser leurs coûts et d'assurer une gouvernance plus cohérente. Les participants ont ainsi indiqué que dans les pays de l'UE, le secret professionnel et la protection des informations commercialement sensibles existaient avant la large reconnaissance des obligations de protection des données apportée par le RGPD lors de son entrée en vigueur. Dans le secteur financier, les organisations étaient déjà soumises à des exigences strictes régissant le traitement, la protection et la divulgation d'informations confidentielles. Le RGPD n'a pas remplacé ces obligations préexistantes, mais a plutôt développé un cadre global traitant spécifiquement du traitement des données personnelles, de la responsabilité, de la transparence et des droits des personnes concernées. Par conséquent, la gouvernance de l'information et la gestion des données étaient déjà ancrées dans le fonctionnement des marchés financiers avant le RGPD, même si le règlement a considérablement élargi le périmètre de la conformité formalisée en matière de protection des données[5].

Notre étude a établi que, malgré son rôle facilitateur et sa reconnaissance croissante en tant qu'actif stratégique, la protection des données n'est pas intégrée de manière cohérente ou distincte dans les processus de gouvernance des organisations. Si les

5 Directive concernant les marchés d'instruments financiers, article 76. Le devoir de secret professionnel s'applique à toutes les personnes qui travaillent pour des autorités compétentes ou des entités auxquelles des tâches sont déléguées, ainsi qu'aux auditeurs et experts mandatés par les autorités compétentes.

activités de conformité – fonction de DPO, contrôles et documentation de conformité, robustesse des systèmes informatiques – réduisent le risque et améliorent la qualité de l'audit, **la protection des données n'est que partiellement présente dans le pilier « gouvernance » des cadres environnementaux, sociaux et de gouvernance (ESG).** Nous avons notamment examiné les cadres ESG largement utilisés dans l'UE et au Royaume-Uni, tels que la directive sur la publication d'informations en matière de durabilité par les entreprises (Corporate Sustainability Reporting Directive - CSRD) et les normes européennes d'information en matière de durabilité (European Sustainability Reporting Standards - ESRS) dans l'UE, ainsi que les Sustainability Reporting Standards (SRS) au Royaume-Uni, qui sont d'application volontaire pour toute entité qui choisit de les utiliser (Commission européenne, 2022) (Département des affaires et du commerce, 2024). Les cadres ESG examinés font généralement référence aux données, sans toutefois mentionner spécifiquement les données personnelles. Les ESRS comportent des règles qui demandent aux organisations comment leurs activités affectent la vie privée des consommateurs et leurs droits en matière de protection des données.

Nous avons constaté que la valeur de la conformité à la protection des données était perçue différemment selon les acteurs ou les types d'organisations. Les DPO sont davantage susceptibles d'en percevoir les avantages, au-delà des obligations législatives et réglementaires. Les conseils d'administration ont tendance à percevoir la valeur de la conformité sous l'angle réputationnel, à travers

les incidents de cybersécurité, les violations de données et les réclamations découlant des demandes d'accès des personnes concernées. À l'instar des DPO, les directions marketing peuvent reconnaître la valeur de la conformité à la protection des données, en réponse à l'importance croissante qu'y attachent les consommateurs et les investisseurs. Bien que ces perceptions distinctes soient courantes, le secteur bancaire pourrait constituer une exception, dans la mesure où les cadres de gestion des risques y sont très matures et où les conseils d'administration considèrent de plus en plus la protection des données comme un facteur bénéfique pour l'activité. L'une des raisons pouvant expliquer l'écart de perceptions entre conseils d'administration, DPO et autres unités opérationnelles réside dans **l'absence d'indicateurs standardisés permettant d'évaluer le niveau de maturité en matière de protection des données.** L'étude a montré que certaines organisations pouvaient intégrer la protection des données dans leur stratégie d'entreprise, laquelle fait l'objet d'un suivi au moyen d'indicateurs clés de performance (KPI), en combinant les enjeux de conformité et de performance opérationnelle, et fait l'objet d'un pilotage au niveau de la direction générale.

Les participants ont également suggéré que les dispositifs de gouvernance des données devraient être orientés vers les résultats, en veillant à ce que les mécanismes de gouvernance, les politiques et les contrôles soient conçus pour soutenir l'atteinte des objectifs clairement définis en matière d'activité, de conformité et d'innovation. Cela pourrait contribuer à combler l'écart entre les difficultés liées à l'évaluation de la valeur des données personnelles et la nécessité d'en démontrer la valeur dans les états comptables. Cela permettrait également de faire le lien de manière concrète entre la conformité en matière de protection des données et les objectifs de l'organisation, qui font régulièrement l'objet d'un suivi et d'une évaluation.

Notre étude a par ailleurs montré que la transparence pouvait témoigner du niveau de maturité d'une organisation dans sa manière de traiter les données personnelles dans le respect de la réglementation et, à ce titre, constituer un avantage concurrentiel. Il existe une certaine transparence dans la manière dont les organisations rendent compte de leur niveau de maturité en matière de conformité à la réglementation sur la protection des données. Toutefois, celle-ci demeure insuffisante, les entreprises ayant tendance à présenter les processus de mise en conformité comme des informations d'ordre opérationnel qui ne sont pas communiquées aux investisseurs ni aux marchés. Par ailleurs, le langage utilisé pour rendre compte du respect de la réglementation en matière de protection des données reste très général et n'offre pas un niveau de transparence suffisant aux consommateurs. Ce constat met en évidence l'émergence d'un **besoin d'indicateurs stratégiques spécifiques, tels que des indicateurs clés de performance (KPI), ou de l'intégration de tels indicateurs dans les rapports ESG,** afin de rendre compte du niveau de maturité en matière de protection des données, tant en interne, auprès des conseils d'administration et des délégués à la protection des données (DPO), qu'en externe, auprès des marchés, des investisseurs, des auditeurs et des consommateurs.

L'Union européenne et le Royaume-Uni ont reconnu l'importance de la cybersécurité sur les marchés financiers et ont désigné les infrastructures bancaires et des marchés financiers comme entités critiques dans le cadre de la directive européenne sur la résilience des entités critiques, tandis que le secteur financier est considéré comme un secteur d'infrastructure nationale critique (Critical National Infrastructure – CNI) au Royaume-Uni (UE 2022/2557, 2022) (National Protective Security Authority, 2026). À la suite de cette désignation, les organisations opèrant dans ces secteurs peuvent s'attendrent à un contrôle accru de leur préparation en matière de cybersécurité. Nos travaux ont montré que, bien que certaines entreprises communiquent sur certains risques de cybersécurité et de protection des données, il n'existe pas d'indicateur standardisé permettant aux marchés et aux investisseurs d'évaluer clairement la qualité de la gouvernance des données. Les répondants ont également indiqué que la protection des données était considérée comme faisant partie intégrante de la politique de cybersécurité dans la plupart des organisations du secteur financier, notamment en raison de l'ampleur des conséquences réputationnelles susceptibles de découler d'incidents cyber.

La gouvernance des données personnelles est abordée sous l'angle de la gestion des risques. L'impact perçu comme le plus significatif des violations en matière de protection des données est la perte de confiance et l'atteinte à la réputation, plutôt que les effets directs des violations de données sur l'évaluation des entreprises, le cours de leurs actions ou leur notation. Malgré la place encore limitée accordée à ces enjeux dans les référentiels ESG, une gouvernance insuffisante des données à caractère personnel peut être mise en évidence dans le cadre des travaux d'audit interne et susciter des préoccupations ou donner lieu à des informations communiquées publiquement lors des assemblées générales des actionnaires. Ainsi, la gouvernance des données est devenue un enjeu important en matière d'audit et de reporting, permettant de limiter les risques liés aux obligations de communication d'informations et à l'atteinte à la réputation.

Notre étude montre que le respect de la réglementation en matière de protection des données influe principalement sur l'évaluation financière des entreprises en cas d'incidents, tels que des violations de données majeures ou des sanctions réglementaires. Cet impact est généralement négatif, lié à la survenance d'un événement, et se manifeste à court terme sur l'évaluation des entreprises ou le cours de leurs actions. L'impact financier des violations de données tend à être de courte durée, varie selon les secteurs et peut être plus marqué pour les grandes entreprises très visibles, principalement en raison des conséquences réputationnelles de la violation. À l'inverse, l'impact des violations de données sur les notations des entreprises dépend de la nature de la violation. Si la plupart des manquements en matière de protection des données n'ont généralement pas d'incidence sur les variations à court terme des notations, **des défaillances graves en matière de protection des données susceptibles d'affecter la résilience financière à long terme peuvent fragiliser le profil de crédit de l'entreprise, entraîner une révision négative de sa perspective de notation** et influer sur sa valorisation par le biais d'une dégradation de sa notation. En outre, les violations de données prolongées susceptibles d'entraîner une interruption des activités ou des services sont plus à même d'affecter la résilience financière des entreprises, ce qui peut à son tour avoir une incidence sur leur évaluation, le cours de leurs actions et leur notation. Les violations de données ont également un impact sur la perception qu'ont les personnes et les consommateurs du partage de leurs données avec les organisations, ainsi que de l'usage des produits et services proposés par des organisations dont les pratiques en matière de gouvernance des données sont insuffisantes. Cela peut, par conséquent, affecter la capacité des organisations à collecter et à utiliser les données à personnelles afin de fournir ou d'améliorer leurs services.

Des cadres de gouvernance efficaces, soutenus par des dispositifs robustes de protection des données, de cybersécurité et de gestion des risques, peuvent renforcer la résilience organisationnelle et le niveau de maturité en matière de cybersécurité. Un meilleur contrôle, un renforcement de la responsabilité et l'amélioration des pratiques de gestion des données permettent aux organisations de mieux identifier, évaluer et atténuer les risques. Les organisations dotées de cadres de gouvernance et de conformité matures, notamment en matière de protection des données, sont généralement mieux à même de se remettre d'incidents, limitant ainsi les atteintes à leur réputation et réduisant les effets potentiels sur leur évaluation, le cours de leurs actions et leurs notations de crédit.

3.1.3 La gouvernance des données comme condition préalable au déploiement de l'IA

Au cours des entretiens, les organisations ont systématiquement identifié l'IA comme une opportunité majeure et comme un élément clé de leur stratégie à long terme et de leurs ambitions de croissance. Les participants ont mis en avant plusieurs cas d'usage émergents déjà déployés, dont le recours à l'IA pour extraire et traiter des informations issues de formulaires et d'autres documents d'entreprise. Les organisations ont également souligné **qu'une gestion efficace des données, une bonne qualité des données et des pratiques rigoureuses en matière de protection des données constituent des prérequis essentiels au déploiement réussi de l'IA.** Ces capacités contribuent à garantir que les données personnelles sont traitées selon une base juridique appropriée, qu'elles demeurent exactes et exploitables, et que les informations pertinentes sont conservées et accessibles à des fins professionnelles légitimes.

Les organisations ont fait valoir que de solides capacités en matière de gestion et de gouvernance des données pouvaient constituer un avantage concurrentiel en permettant une utilisation efficace de l'IA et en transformant la conformité, d'une obligation réglementaire en un actif stratégique. Sans des données fiables, correctement gérées et soumises à une gouvernance appropriée, les organisations peuvent avoir des difficultés à tirer pleinement parti de la valeur des technologies de l'IA.

Les organisations ont estimé que de solides capacités en matière de gestion et de gouvernance

des données pouvaient constituer un avantage concurrentiel en permettant une utilisation efficace de l'IA et en transformant la conformité réglementaire, d'une obligation réglementaire en un atout stratégique. Sans données fiables, correctement gérées et soumises à une gouvernance appropriée, les organisations peuvent avoir des difficultés à tirer pleinement parti de la valeur des technologies d'IA.

Les participants aux entretiens ont indiqué que les organisations européennes restaient dépendantes d'infrastructures numériques et de fournisseurs de technologies non européens, en raison de la structure de la chaîne d'approvisionnement du marché des développeurs d'IA. Cette dépendance peut limiter leur capacité à exploiter pleinement la valeur des données à caractère personnel en tant qu'actif stratégique au service de l'innovation et du développement de l'IA.

Pour certaines organisations, notamment les établissements financiers et les autorités de régulation, la confiance dans la sécurité constitue un facteur de différenciation essentiel. À mesure que les organisations intensifient le déploiement de solutions d'IA, les participants ont souligné qu'une solide conformité en matière de protection des données, la transparence et des dispositifs de gouvernance efficaces sont indispensables pour préserver et renforcer la confiance des clients, en particulier lorsque des données personnelles sont utilisées dans des processus liés à l'IA. Comme indiqué plus haut, l'un des principaux constats de l'étude est un décalage entre la perception qu'ont les conseils d'administration et les DPO du rôle de la conformité en matière de protection des données. **Le déploiement de l'IA pourrait offrir aux DPO une occasion de démontrer clairement la valeur ajoutée d'une bonne gouvernance,** au-delà du strict respect des exigences légales, en mettant en évidence les bénéfices qu'elle peut apporter à la croissance des organisations et à la réalisation leurs priorités stratégiques.

Des dispositifs de gouvernance responsables deviennent de plus en plus importants avec l'adoption de l'IA agentique au sein des organisations, c'est-à-dire de systèmes d'intelligence artificielle qui vont au-delà de la simple réponse aux requêtes et sont capables d'exécuter des tâches de manière autonome. Les participants exerçant des fonctions de support aux services financiers ont indiqué suivre de près l'évolution de ces systèmes, car ceux-ci semblent amplifier les risques liés à la cybersécurité, notamment parce que l'utilisation de systèmes agentiques automatisés sans supervision humaine multiplie les vulnérabilités telles que l'injection de prompts et l'empoisonnement des données.

L'enquête quantitative, menée auprès du secteur privé, révèle une adoption rapide des outils d'IA au sein des entreprises interrogées : plus de deux tiers (69 %) utilisent déjà des outils d'IA sous licence entreprise pour augmenter la productivité, signe que l'IA fait désormais partie intégrante du quotidien professionnel. Une étude menée au Royaume-Uni a également établi que le recours à des outils d'IA pour le traitement des données personnelles était passé de 6 % en 2024 à 8 % en 2025 puis 14 % en 2026 (ICO, 2026).

L'enquête menée auprès des organisations françaises montre

également que l'adoption de l'IA s'accompagne de **niveaux variables de sensibilisation et de compréhension :** 18 % des répondants bloquent délibérément les outils publics d'IA générative pour des motifs de confidentialité et de propriété intellectuelle. Un quart des répondants (26 %) connectent déjà l'IA à leurs bases de données internes, tandis que 11,6 % déploient des agents conversationnels ou des assistants pour une utilisation interne ou en contact avec les clients. À la pointe de l'innovation, 5 % commercialisent leurs propres modèles d'IA générateurs de revenus. Bien que les organisations diffèrent sensiblement dans leur compréhension et leur niveau de maturité en matière de gouvernance de l'IA, de gestion des risques et de respect des exigences de conformité, nombre d'entre elles déclarent avoir mis en place des mesures spécifiques de protection des données, telles que le recours à des outils « fondés sur une IA existante avec anonymisation et filtrage des données», le déploiement d'une « version personnalisée et sécurisée d'un agent conversationnel, conçue pour répondre à des exigences spécifiques » ou encore l'utilisation de systèmes d'IA juridiques à accès restreint. Les organisations formalisent également leurs règles au moyen de dispositifs telles que des chartes sur l'IA, des « sections encadrant l'utilisation de l'IA », des programmes pilotes limités à un groupe restreint de collaborateurs avant un déploiement à grande échelle, ou encore le blocage des outils jugés problématiques.

L'enquête quantitative menée auprès des responsables de traitement français a également établi (voir l'annexe statistique) que l'adoption de l'IA est corrélée à des facteurs financiers, tels que la taille de l'entreprise (mesurée en chiffre d'affaires), et moins à la dépendance aux données, ce qui suggère que la capacité à financer des projets d'IA et à y consacrer du temps est déterminée par d'autres facteurs. **Un lien direct a également été établi entre l'adoption d'applications d'IA avancées (IA connectée à des bases de données internes, agents conversationnels destinés aux clients ou des modèles d'IA commercialisés) et l'intégration des risques liés aux données dans les évaluations financières (notations de crédit, évaluation des fusions-acquisitions ou coût du capital).** Ces résultats indiquent que certaines entreprises qui investissent dans l'IA commencent également à prendre en compte les risques associés aux données.

3.2 Traitement comptable et exposition financière liés aux enjeux de données

3.2.1 Points de vue des parties prenantes sur les données et la conformité en matière de protection des données dans les états financiers

Les entretiens menés avec des commissaires aux comptes et des régulateurs apportent un éclairage précieux sur la manière dont les questions de données sont progressivement intégrées à l'évaluation des risques financiers, tout en restant ancrées dans les objectifs traditionnels de la fonction d'audit.

Une première observation importante concerne le niveau de préparation des organisations. Plusieurs répondants ont souligné que de nombreuses organisations ne disposent pas encore pleinement des moyens nécessaires pour évaluer et

analyser les implications financières de la protection des données. La coordination en interne demeure limitée, les différents services – notamment les services juridiques, la conformité, l'informatique et la finance – abordant souvent cette question sous des angles distincts. Il en résulte que la traduction des risques liés aux données en indicateurs financiers reste fragmentée et encore peu développée.

Du point de vue de l'audit, la protection des données n'est pas évaluée comme un objectif de conformité à part entière, mais plutôt au regard de son incidence potentielle sur l'information financière. Les auditeurs ont souligné que leur principale responsabilité consistait à identifier et évaluer les risques d'anomalies significatives dans les états financiers. Dans ce contexte, les enjeux liés à la protection des données interviennent principalement par deux canaux. Tout d'abord, **ils sont liés à la qualité des données,** qui constitue un fondement de la fiabilité des informations comptables. Deuxièmement, **ils relèvent du champ d'application du** « non-respect des dispositions légales et réglementaires » (**NOCLAR** – Non-Compliance with Laws and Regulations), lorsque des manquements aux règles de protection des données peuvent entraîner des conséquences financières telles que des amendes, des perturbations opérationnelles ou une dépréciation des actifs. Cette approche est conforme à la norme ISA 250 (Prise en compte des textes légaux et réglementaires dans un audit d'états financiers), qui exige des auditeurs qu'ils obtiennent des éléments probants suffisants et appropriés concernant le respect des dispositions légales et réglementaires ayant une incidence directe ou indirecte sur les états financiers, et qu'ils évaluent si les cas de non-respect sont susceptibles d'entraîner des anomalies significatives (IAASB, 2016).

Un défi majeur, relevé dans l'ensemble des entretiens, réside dans la difficulté de traduire des caractéristiques qualitatives de conformité en risques financiers quantifiables. Les dispositifs de protection des données sont souvent conçus sous un angle juridique et ne fournissent pas directement les données nécessaires à l'évaluation financière ou la mesure des risques. En pratique, **les auditeurs et les professionnels de la finance s'appuient sur des analyses fondées sur des scénarios en évaluant l'impact financier potentiel des manquements à la réglementation,** notamment les sanctions, les interruptions d'activité, les atteintes à la réputation ou la diminution de l'exploitabilité des données.

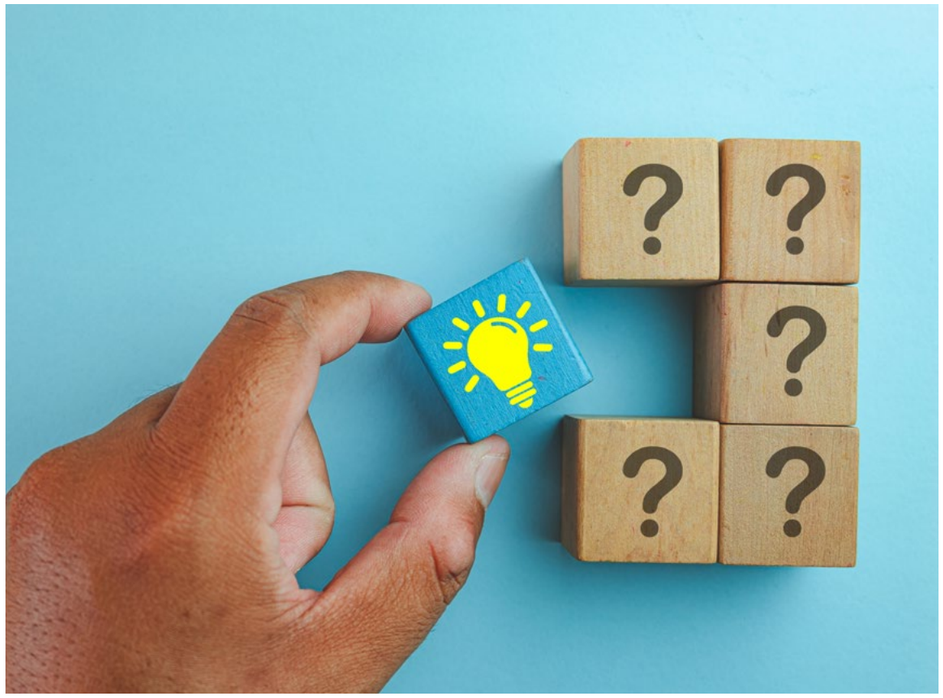
Au-delà de ces impacts directs, les répondants ont souligné que les risques liés à la protection des données peuvent également influencer des paramètres d'évaluation financière, en particulier **le coût moyen pondéré du capital** (WACC)[6]. Une incertitude accrue quant à la licéité et à la pérennité de l'utilisation des données peut conduire les investisseurs et les professionnels de l'évaluation à exiger des rendements plus élevés, augmentant ainsi le coût de financement du capital de l'entreprise.

Ce mécanisme constitue un canal de transmission essentiel entre les risques liés à la protection des données et les évaluations financières, puisqu'il amplifie l'effet d'une diminution des flux de trésorerie futurs estimés.

Ce double effet est particulièrement marqué dans les modèles d'affaires fondés sur les données, où la valeur est intrinsèquement liée à l'utilisation des données. **Lorsque des actifs de données sont affectés par des problèmes de conformité, leur valeur économique peut être significativement dégradée.** Dans certains cas, il a été explicitement soutenu qu'un actif qui ne peut pas être utilisé légalement ne devrait pas être considéré comme ayant une valeur marchande. Cette question est particulièrement pertinente pour les actifs constitués de données personnelles : les données collectées, traitées ou conservées en violation de la législation applicable en matière de protection des données, comme le RGPD ou la loi du Royaume-Uni, peuvent devenir inutilisables à des fins commerciales. Dans de telles circonstances, les limitations juridiques attachées à l'actif affectent directement sa capacité à générer des avantages économiques futurs et, par conséquent, sa valeur économique.

Du point de vue comptable, les interactions entre la valeur de la conformité en matière de protection des données et sa prise en compte dans l'information financière se reflètent dans plusieurs dispositions comptables.

Pour comprendre les effets de ces dynamiques, ce rapport s'est concentré principalement sur leurs implications au regard des normes internationales d'information



6 Le coût moyen pondéré du capital ou WACC est le coût moyen du financement par emprunt et par capitaux propres d'une entreprise, pondéré par leurs proportions dans la structure du capital, et est couramment utilisé comme taux d'actualisation dans l'évaluation des entreprises et le test de dépréciation selon l'IAS 36.

financière (IFRS) pertinentes, notamment IAS 38 (Immobilisations incorporelles), IAS 36 (Dépréciation d'actifs) et IFRS 3 (Regroupements d'entreprises).

Les normes examinées ont été identifiées à partir des entretiens qualitatifs menés avec des auditeurs, des consultants et des autorités de surveillance, qui ont mis en évidence l'importance des questions comptables liées aux listes de clients et aux bases de données clients, en particulier dans les regroupements d'entreprises[7] (par exemple : acquisition ou fusion) et des exercices d'évaluation. En particulier, une détérioration des avantages futurs attendus peut entraîner une dépréciation du goodwill et des immobilisations incorporelles selon la norme IAS 36 (Dépréciation d'actifs). Les risques réglementaires peuvent également donner lieu à des provisions au titre de l'IAS 37 lorsque les obligations sont probables et mesurables. Dans le contexte des acquisitions, la valeur liée aux données est souvent intégrée au goodwill dans le cadre de l'allocation du prix d'acquisition. Toute dégradation ultérieure des synergies attendues, notamment celles liées à l'exploitation des données, peut alors entraîner la comptabilisation de pertes de valeur. En outre, toute variation du taux d'actualisation, reflétant une augmentation du niveau de risque, affecte directement la valeur calculée.

Du point de vue de la gouvernance et de la certification, les répondants ont indiqué que les auditeurs prennent en compte l'environnement de contrôle dans son ensemble, notamment les contrôles internes, les systèmes informatiques et les structures organisationnelles. Des éléments tels que la présence d'un DPO, les travaux d'audit interne portant sur les cadres juridiques applicables à la protection des données, ainsi que l'existence de certifications, de codes de conduite ou d'autres dispositifs de conformité reconnus, peuvent constituer des éléments de garantie supplémentaires, dans la mesure où ils témoignent de la mise en place de mécanismes structurés de conformité. Ces éléments ne constituent toutefois qu'un aspect parmi d'autres et ne dispensent pas des procédures d'audit, leur pertinence dépendant en définitive de leur capacité à atténuer les risques d'anomalies significatives.

Du point de vue des normes comptables, les répondants n'ont pas identifié de lacune fondamentale dans le cadre existant. Les normes IFRS actuelles, en particulier IAS 36, IAS 37, IAS 38 et IFRS 3, ont été considérées suffisamment larges pour appréhender de la protection des données et des risques associés.

Toutefois, l'application de ces normes repose sur un degré élevé de jugement professionnel, notamment compte tenu de l'évolution constante des risques liés aux données. **Le principal enjeu ne semble donc pas résider dans l'absence de règles, mais plutôt dans leur interprétation et leur application cohérente en pratique.**

7 Un regroupement d'entreprises est « une transaction ou un autre événement par lequel un acquéreur obtient le contrôle d'une ou de plusieurs entreprises » (IFRS 3, annexe A).

3.2.2 Les actifs de données et la protection des données dans l'information financière

Cette section examine les implications comptables des thématiques liées aux données en analysant la manière dont les obligations de conformité sont prises en compte dans le cadre des principales normes et procédures comptables. À l'aide d'exemple pratiques elle illustre leur incidence sur les états financiers et les traitements comptables. L'analyse se concentre sur IAS 38 (Immobilisations incorporelles), IFRS 3 (Regroupements d'entreprises) et IAS 36 (Dépréciation des actifs), ces normes fournissant le cadre à la comptabilisation, à l'évaluation et aux tests de la dépréciation des actifs liés aux données.

Un objectif essentiel consiste également à d'identifier les circonstances dans lesquelles les bases de données peuvent être comptabilisées en tant qu'actifs ainsi que la manière dont les exigences en matière de protection des données peuvent influencer leur évaluation et leur traitement comptable. La comparaison avec les référentiels comptables nationaux généralement admis (Generally Accepted Accounting Principles, GAAP), tels que le Plan comptable général (PCG) en France, les normes luxembourgeoises et le référentiel britannique (UK GAAP), met davantage en évidence les différences de traitement de réalités économiques similaires selon les juridictions.

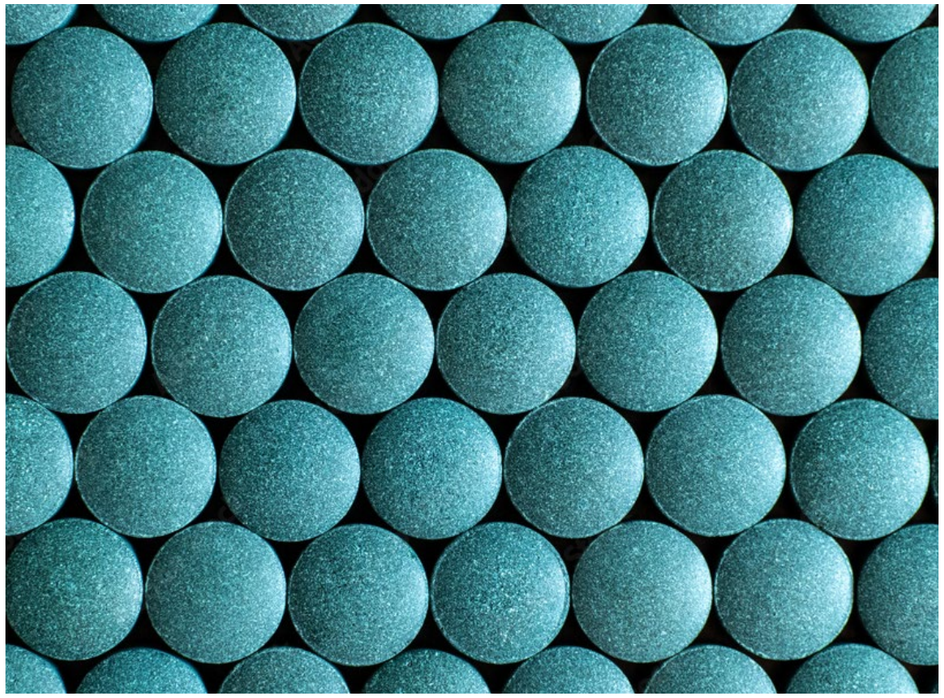
La norme IAS 37 (Provisions, passifs

éventuels et actifs éventuels) n'est pas examinée en détail, le rapport portant principalement sur la comptabilisation, l'évaluation et la dépréciation des actifs liés aux données plutôt que sur le traitement comptable des obligations, telles que les amendes ou les risques de contentieux.

La reconnaissance croissante des données comme un actif économique

La littérature académique et professionnelle récente souligne de plus en plus l'importance stratégique et économique des données, soulevant des interrogations quant à la capacité des référentiels comptables existants à en appréhender correctement la valeur. Alors que les données sont devenues un facteur essentiel de la performance des entreprises, plusieurs auteurs et institutions ont fait valoir **qu'elles devraient être considérées et gérées plus explicitement comme des actifs.**

Un rapport de Deloitte (2025) souligne que les données sont devenues une ressource critique pour de nombreuses organisations et présente des exemples d'entreprises qui comptabilisent les actifs liés aux données dans leur information financière, lorsque ces actifs sont considérés comme fondamentaux pour leur modèle économique. Le rapport fait valoir que, dans de nombreux cas, les données génèrent des avantages économiques significatifs grâce aux gains d'efficacité opérationnelle, à l'amélioration de la prise de décision, à l'innovation et à la création de nouvelles sources de revenus. En conséquence, le rapport suggère que les données devraient être évaluées selon des méthodes de valorisation couramment appliquées à d'autres



immobilisations incorporelles, à savoir l'approche par les flux futurs, l'approche par les coûts et l'approche par le marché, telles qu'examinées dans la revue de littérature. Ces méthodes visent à estimer la valeur économique des données en fonction des avantages futurs attendus, des coûts engagés pour les créer ou les remplacer, ou de transactions de marché comparables.

En plus de mettre en évidence la valeur des données, les auteurs introduisent le concept de « **dette de données** » (data debt). Ce concept traduit l'idée selon laquelle, si des actifs de données gérés efficacement peuvent créer une valeur substantielle et soutenir la croissance de l'entreprise, une mauvaise gouvernance des données peut, à l'inverse, entraîner des coûts importants pour les organisations. Ces coûts peuvent résulter de problèmes de qualité des données, d'incidents de cybersécurité, de violations de données, de sanctions réglementaires ou de manquements aux exigences en matière de protection des données et de la vie privée. Par conséquent, les données ne devraient pas seulement être considérées comme une source potentielle de création de valeur, mais également comme une source de risques nécessitant des mécanismes appropriés de gestion et de gouvernance.

De même, l'Institute of Chartered Accountants in England and Wales examine le rôle croissant des données dans les modèles économiques modernes et s'interroge sur la capacité des normes comptables existantes à refléter correctement leur importance économique (ICAEW, 2025). Le rapport met en évidence le **décalage croissant entre la valeur générée par les activités fondées sur les données et la reconnaissance limitée des actifs de données générés en interne dans les états financiers.** Alors que les entreprises s'appuient de plus en plus sur les données pour créer des avantages concurrentiels, mieux comprendre leurs clients, développer leurs capacités d'innovation et améliorer leur efficacité opérationnelle, le rapport suggère que les référentiels comptables actuels pourraient ne pas rendre pleinement compte des ressources qui contribuent à la création de valeur de l'entreprise.

La recherche académique s'est également intéressée aux difficultés liées à l'évaluation et à la comptabilisation des données (Blycha et al., 2026). Les auteurs proposent un cadre structuré d'évaluation visant à évaluer les données d'entreprise conformément aux normes comptables existantes. L'article soutient que la difficulté à évaluer les données de manière simple et fiable entraîne des erreurs d'évaluation et des distorsions dans l'allocation des ressources. Le cadre prend en compte les situations dans lesquelles les données ont été qualifiées soit d'immobilisations incorporelles selon IAS 38, soit, dans certains contextes économiques, de stocks au sens d'IAS 2. Cette approche alimente le débat en cours concernant le traitement comptable approprié des données et fournit une méthodologie susceptible de combler l'écart entre la valeur économique et les exigences de reporting financier.

Pris dans leur ensemble, ces développements illustrent l'existence d'un consensus croissant selon lequel les données constituent une ressource importante pour l'entreprise, dont l'importance économique dépasse leur traitement traditionnel dans

les états financiers. Bien que des normes comptables telles qu'IAS 38 continuent d'imposer des critères de comptabilisation stricts, les récentes contributions professionnelles et académiques suggèrent que les données présentent de plus en plus de caractéristiques associées à des immobilisations incorporelles de valeur et **pourraient à l'avenir nécessiter des approches plus sophistiquées en matière d'évaluation et de reporting.**

3.2.3 Résultats quantitatifs

Les résultats de l'enquête menée auprès d'organisations françaises indiquent que la comptabilisation des bases de données dans les états financiers demeure limitée et hétérogène. Parmi les répondants ayant exprimé une opinion sur le sujet, une majorité a indiqué que leurs bases de données ne sont pas comptabilisées dans les états financiers (38 %). Lorsqu'elles sont comptabilisées, **l'approche dominante repose sur les coûts**, principalement par la capitalisation des coûts de développement informatique et de création des bases de données en tant qu'immobilisations incorporelles, pour près d'un tiers des répondants (28 %). Seule une faible proportion des répondants (5 %) a indiqué que les bases de données sont reflétées par le goodwill résultant d'opérations d'acquisition. Ces résultats suggèrent que les pratiques comptables actuelles ont tendance à se concentrer sur les coûts engagés pour créer des bases de données, plutôt que sur la valeur économique sous-jacente générée par les actifs de données.

Conformément aux constats précédents, les résultats de l'enquête suggèrent que même les données acquises ne sont encore que rarement traitées comme un actif distinct. Plus de la moitié des répondants (53 %) ont indiqué qu'aucune évaluation spécifique n'était réalisée pour les données acquises. Néanmoins, **certaines pratiques de comptabilisation commencent à émerger** : 18 % des répondants ont déclaré comptabiliser les données acquises en tant qu'immobilisations incorporelles distinctes au bilan, tandis que 14 % ont indiqué que leur valeur est prise en compte indirectement dans le goodwill, sans être identifiée séparément. Les autres réponses révèlent un degré important d'incertitude concernant le traitement comptable des données acquises, soulignant que la comptabilisation des données en tant qu'actifs demeure une pratique en cours d'évolution et un domaine dans lequel les connaissances et les méthodes comptables pourraient encore être développées.

3.2.4 Comptabilisation, évaluation et dépréciation des bases de données au titre d'IAS 38, IFRS 3 et IAS 36

Sur la base des considérations qui précèdent, cette section se concentre sur l'analyse d'IAS 38 (Immobilisations incorporelles), d'IFRS 3 (Regroupements d'entreprises) et d'IAS 36 (Dépréciation d'actifs), ces normes constituant le cadre le plus pertinent pour examiner la comptabilisation, la mesure et l'évaluation ultérieure des bases de données clients.

Par ailleurs, l'analyse adopte une approche comparative en faisant référence au PCG français, aux normes comptables luxembourgeoises et au référentiel britannique (FRS 102). Cette comparaison permet de

mettre en évidence les différences de traitement comptable des immobilisations incorporelles liées aux clients selon les différents référentiels comptables.

Enfin, l'analyse s'appuie sur un exemple pratique figurant à l'annexe B, illustrant la manière dont les bases de données clients sont comptabilisées, évaluées et, le cas échéant, soumises à un test de dépréciation dans le contexte d'une transaction, établissant ainsi un lien entre les principes théoriques et les pratiques réelles en matière d'évaluation et de comptabilisation.

Comptabilisation des bases de données au titre d'IAS 38

IAS 38, adoptée en 2001 et publiée en 2004, régit la comptabilisation, l'évaluation et l'amortissement des immobilisations incorporelles. Selon cette norme, une immobilisation incorporelle n'est comptabilisée que s'il est probable que les avantages économiques futurs attendus qui lui sont attribuables bénéficieront à l'entité et si son coût peut être évalué de manière fiable[8]. En pratique, ces critères sont généralement remplis pour les immobilisations incorporelles acquises séparément, dans la mesure où le prix d'achat reflète les anticipations des acteurs du marché concernant les avantages économiques futurs.

En plus de ces critères de comptabilisation, IAS 38 exige que l'actif soit identifiable[9] et contrôlé par l'entité[10]. Une immobilisation incorporelle est identifiable lorsqu'elle

8 IAS 38, paragraphe 21
9 IAS 38, paragraphe 12
10 IAS 38, paragraphe 13

est soit séparable, soit issue de droits contractuels ou légaux. Cette distinction est particulièrement pertinente pour les bases de données client, généralement considérées comme séparables dès lors qu'elles peuvent par exemple être transférées, concédées sous licence ou échangées d'une autre manière, sous réserve du respect de la réglementation relative à la protection des données. La notion de contrôle implique que l'entité soit en mesure d'obtenir les avantages économiques futurs découlant de l'actif, sur le fondement juridique approprié au regard de la réglementation en matière de protection des données.

IAS 38 établit également une **distinction claire entre les immobilisations incorporelles acquises et celles générées en interne**[11]. Le goodwill généré en interne ne peut pas toujours être comptabilisé en tant qu"actif, car les critères de contrôle et d'identifiabilité ne peuvent pas être démontrés aisément. Par ailleurs, IAS 38 exclut explicitement les « fichiers client » de la comptabilisation en tant qu'immobilisations incorporelles (§632), même si tous les jeux de données ne sont pas constitués de bases de données client.

Comptabilisation des bases de données internes en tant qu'immobilisations incorporelles au titre d'IAS 38

Bien que les bases de données générées en interne ne soient généralement pas comptabilisées en tant qu'immobilisations incorporelles, certaines circonstances peuvent leur permettre de satisfaire aux critères de comptabilisation établis par IAS 38 (Immobilisations incorporelles). **Trois situations sont particulièrement pertinentes :**

- **La présence de coûts de développement informatique liés à la création de bases de données ;**
- **Les bases de données ou jeux de données protégés par des droits de propriété intellectuelle ou d'autres droits légaux ; et**
- **Les bases de données internes spécialisées (structurées).**

Dans ces situations particulières, les bases de données développées pour un usage interne peuvent satisfaire aux critères de comptabilisation et par conséquent, être qualifiées d'immobilisations incorporelles.

i. Présence de coûts de développement informatique liés à la création de bases de données

Un aspect essentiel d'IAS 38 est la distinction entre la phase de recherche et la phase de développement d'une immobilisation incorporelle générée en interne. Les dépenses engagées au cours de la phase de recherche doivent être comptabilisées en charges au fur et à mesure qu'elles sont encourues, car les avantages économiques futurs ne peuvent pas encore être démontrés. À l'inverse, les dépenses de développement peuvent être inscrites à l'actif lorsque l'entité est en mesure de démontrer la faisabilité technique du projet, son intention d'achever et d'utiliser l'actif, sa capacité à générer des avantages économiques futurs, la disponibilité de ressources adéquates pour mener le projet à son terme, ainsi que sa capacité à évaluer de manière fiable les coûts attribuables à l'actif. Ces exigences sont énoncées au paragraphe 57 d'IAS 38 et constituent le fondement de la comptabilisation à l'actif des bases de données développées en interne.

Pour les projets de développement de bases de données, les dépenses pouvant généralement être comptabilisées à l'actif comprennent les coûts directement attribuables à la création de l'actif et à sa préparation en vue de son utilisation prévue. Ces coûts peuvent notamment inclure les salaires des développeurs logiciels et des ingénieurs bases de données, les honoraires de consultants externes liés à la conception et au développement du système, les activités de test, ainsi que les autres dépenses de mise en œuvre directement attribuables. Conformément à la norme IAS 38, l'actif est initialement évalué à son coût, lequel comprend uniquement les dépenses pouvant être directement rattachées à la création de la base de données.

À l'inverse, certains coûts ne peuvent pas être inclus dans la valeur comptable de la base de données et doivent être comptabilisés en charges au moment où ils sont engagés. Il s'agit notamment des coûts de formation des utilisateurs, des frais généraux administratifs, des activités de maintenance et des dépenses engagées au cours des études préliminaires ou des études de faisabilité. L'IAS 38 exclut expressément ces dépenses de la capitalisation, car elles ne contribuent pas directement à la création d'une immobilisation incorporelle susceptible de générer des avantages économiques futurs.

Par conséquent, selon les normes IFRS, le traitement comptable des coûts de création d'une base de données dépend du fait que les dépenses satisfassent ou non aux critères de comptabilisation applicables aux immobilisations incorporelles générées en interne au titre l'IAS 38. **Lorsque les critères relatifs à la phase de développement sont remplis, les coûts éligibles sont comptabilisés à l'actif puis amortis sur la durée d'utilité de l'actif.** Dans le cas contraire, les dépenses sont immédiatement comptabilisées en résultat. Cette approche garantit que seuls les investissements informatiques dont on s'attend à ce qu'ils génèrent des avantages économiques futurs sont comptabilisés en tant qu'actifs au bilan.

ii. Droits de propriété intellectuelle attachés aux bases de données

L'existence de droits de propriété intellectuelle associés à une base de données peut faciliter le respect des exigences d'IAS 38 relatives à l'identifiabilité et au contrôle. Des droits légaux tels que les droits d'auteur, les droits sui generis sur les bases de données, les licences ou les droits exclusifs d'utilisation peuvent démontrer qu'une base de données constitue une ressource identifiable, distincte de l'entité. Ces droits permettent d'établir que la base de données peut être distinguée des autres actifs et peut, par conséquent, satisfaire aux critères d'identifiabilité. Par d'exemple, le Code de la propriété intellectuelle français comporte une disposition créant un droit sui generis sur une base de données lorsqu'un « investissement substantiel » lui a été

11 IAS 38, paragraphes 10 et 18–23, qui établissent une distinction entre les actifs incorporels acquis et ceux générés en interne, ces derniers étant soumis à des restrictions importantes en matière de comptabilisation, notamment en ce qui concerne le goodwill généré en interne et les éléments similaires.

consacré[12]. D'autres bases de données peuvent relever du droit d'auteur au titre de la directive européenne 96/9/CE concernant la protection juridique des bases de données.

En outre, **la protection juridique renforce la capacité de l'entité à contrôler les avantages économiques futurs découlant de la base de données.** En limitant l'accès des tiers et en conférant des droits exclusifs permettant d'utiliser, d'exploiter, de concéder sous licence ou de commercialiser les informations sous-jacentes, ces droits permettent à l'entité de tirer des avantages économiques de la base de données tout en empêchant les tiers d'en faire autant.

Par conséquent, les bases de données protégées par des droits de propriété intellectuelle peuvent être qualifiées d'immobilisations incorporelles au titre d'IAS 38 lorsque ces droits établissent à la fois leur identifiabilité et le contrôle. L'existence d'une protection juridique ne suffit toutefois pas à elle seule. L'entité doit également démontrer que la base de données devrait générer des avantages économiques futurs et que son coût peut être évalué de manière fiable, conformément aux critères généraux de comptabilisation prévu par l'IAS 38.

iii. Bases de données et jeux de données internes spécialisés

En plus des bases de données bénéficiant d'une protection juridique, certaines bases de données ou certains jeux de données spécialisés développés en interne peuvent satisfaire aux critères de comptabilisation de l'IAS 38. Cela peut notamment être le cas **lorsque des efforts de développement significatifs ont été consentis pour collecter, enrichir, structurer,** nettoyer, valider ou organiser des données, créant ainsi une ressource génératrice de valeur économique pour l'entité.

On peut citer, à titre d'exemples, les jeux de données propriétaires utilisés pour l'entraînement des modèles d'intelligence artificielle, les bases de données de recherche en santé faisant l'objet d'une sélection et d'une structuration spécifiques, les bases de données géospatiales, les référentiels de données techniques ou scientifiques, ainsi que d'autres jeux de données spécialisés développés à des fins d'exploitation commerciale ou dans le cadre d'objectifs stratégiques pour l'entreprise. Les bases de données faisant l'objet de licences exclusives ou procurant à l'entité un avantage concurrentiel unique sont particulièrement pertinentes dans ce contexte.

Lorsque ces bases de données sont identifiables, contrôlées par l'entité, susceptibles de générer des avantages économiques futurs probables, et que les coûts de développement associés peuvent être évalués de façon fiable, elles peuvent être comptabilisées en immobilisations incorporelles au titre de l'IAS 38. Chaque cas doit néanmoins faire l'objet d'une analyse individuelle, en tenant compte des caractéristiques propres à la base de données concernée et des éléments disponibles pour démontrer le respect des critères de comptabilisation prévu par la norme.

Les listes de clients générées en interne[13] sont expressément exclues de la comptabilisation à l'actif, car elles ne peuvent être distingués de la valeur globale de l'entreprise et ne satisfont donc aux critères d'identifiabilité et d'évaluation fiable. Par conséquent, de nombreuses dépenses indirectes liées aux données, telles que les coûts engagés pour améliorer la gouvernance des données, renforcer leur qualité, ou assurer le respect à la réglementation sur la protection des données, sont comptabilisées en charges au fur et à mesure qu'elles sont engagées[14], car elles ne satisfont pas aux critères de comptabilisation.

Bien qu'IAS 38 définisse le cadre général applicable à la comptabilisation des bases de données client, des exigences supplémentaires s'appliquent lorsque de tels actifs sont acquis dans le cadre d'un regroupement d'entreprises [15].

Comptabilisation et évaluation initiale dans les regroupements d'entreprises au titre d'IFRS 3

Lorsqu'une base de données clients est acquise dans le cadre d'un regroupement d'entreprises, la norme IFRS 3 « Regroupements d'entreprises » s'applique. L'IFRS 3 repose sur la méthode de l'acquisition, qui impose d'identifier et d'évaluer les actifs acquis et les passifs repris à leur juste valeur à la date d'acquisition. Pour être comptabilisés, ces éléments doivent répondre aux définitions des actifs et des passifs énoncées dans le Cadre conceptuel de l'information financière et faire partie intégrante de l'opération de regroupement d'entreprises[16].

Dans ce contexte, IFRS 3 étend l'application de la norme IAS 38 en exigeant que toutes les immobilisations incorporelles identifiables soient comptabilisées séparément du goodwill, même si elles n'étaient pas auparavant comptabilisées par l'entreprise acquise[17]. Comme mentionné précédemment, conformément à l'IAS 38, l'identifiabilité est établie lorsqu'un actif est séparable ou résulte de droits contractuels ou légaux. En conséquence, même les fichiers clients, les jeux de données utilisateurs et les immobilisations incorporelles liées aux clients peuvent fréquemment être comptabilisés à leur juste valeur à la date d'acquisition, y compris lorsqu'ils ont été développés en interne.

Cette approche peut conduire à comptabiliser des actifs qui ne figuraient pas auparavant dans les états financiers de l'entreprise acquise, ce qui revêt une importance particulière dans les environnements fondés sur la donnée. Une base de données client, acquise dans le cadre d'une telle opération, peut ainsi être qualifiée d'immobilisation incorporelle

12 article L. 341-1 du code de la propriété intellectuelle.
13 IAS 38, paragraphe 63.
14 IAS 38, paragraphes 21 et 68–69, qui établissent que les dépenses qui ne remplissent pas les critères de comptabilisation des immobilisations incorporelles, en particulier les coûts générés en interne, doivent être comptabilisées en tant que charges au moment où elles sont encourues.
15 IFRS 3, paragraphes 10 et B31–B34, qui exigent que l'acquéreur comptabilise les immobilisations incorporelles identifiables séparément du goodwill si elles répondent à la définition d'une immobilisation incorporelle et peuvent être évaluées de manière fiable.
16 Cadre conceptuel pour l'information financière, paragraphes 4.3–4.4, qui définit les actifs et les passifs, et IFRS 3, paragraphe 10, qui exige la comptabilisation d'actifs et de passifs identifiables répondant à ces définitions dans un regroupement d'entreprises.
17 IFRS 3, paragraphes 10 et B31–B32.

s'il est probable qu'elle génère des avantages économiques futurs. Sa durée de vie utile[18] est déterminée en fonction de la période pendant laquelle ces avantages sont censés être générés.

Évaluation du goodwill au titre d'IFRS 3

Selon IFRS 3, le goodwill correspond à l'excédent de la valeur attribuée à une entreprise acquise, y compris les éventuels intérêts ne donnant pas le contrôle et les participations antérieurement détenues, sur la juste valeur nette des actifs identifiables acquis et des passifs repris. Il reflète les avantages économiques futurs résultants d'actifs qui ne peuvent pas être identifiés individuellement et comptabilisés séparément.

Dans un contexte lié aux données, le goodwill peut incorporer la valeur associée aux synergies résultant de l'utilisation combinée des données, de l'amélioration des capacités d'analyse ou du développement de nouveaux services fondés sur la donnée, sous réserve du respect des cadres réglementaires applicables.

IFRS 3 prévoit également une période d'évaluation postérieure à la date d'acquisition, pendant laquelle les montants provisionnels initialement comptabilisés peuvent être ajustés[19]. Cette période permet à l'acquéreur d'affiner l'évaluation des actifs et des passifs, y compris des bases de données clients. Les ajustements sont limités aux informations relatives aux faits et circonstances qui existaient à la date d'acquisition et sont comptabilisés rétrospectivement, ce qui peut entraîner des ajustements correspondant du goodwill.

Protection des données, propriété et amortissement des actifs de données

Comme indiqué précédemment, selon IAS 38, la comptabilisation en tant qu'immobilisations incorporelles ne constitue pas la règle générale applicable aux bases de données client générées en interne, car il est difficile de démontrer que l'ensemble des critères de comptabilisation sont remplis. En revanche, les bases de données client acquises, soit séparément, soit dans le cadre d'un regroupement d'entreprises, peuvent satisfaire à ces critères.

En conséquence, les fichiers de clients développés en interne, les données relatives aux utilisateurs ou aux clients accumulées en interne et, plus largement, les dépenses liées aux données qui ne peuvent être dissociées des activités courantes de l'entité peuvent être comptabilisées en charges.

Un jeu de données comptabilisé en tant qu'actif et répondant aux critères d'IAS 38 peut faire l'objet d'un amortissement. Après la comptabilisation initiale, conformément à IAS 38, les immobilisations incorporelles ayant une durée de vie utile finie sont amortis systématiquement sur leur durée de vie utile estimée[20]. La durée de vie utile doit être déterminée en fonction de la période pendant laquelle des avantages économiques sont attendus du jeu de données.

18 IAS 38 définit la durée de vie utile comme la période pendant laquelle une entité s'attend à pouvoir utiliser un actif, ou le nombre d'unités de production ou similaires que l'entité s'attend à obtenir de l'actif.

19 IFRS 3, paragraphes 45 à 49.

20 IAS 38, paragraphes 88–89 et 97

Sur ce sujet, il est souvent avancé que la durée de vie utile d'un jeu de données est relativement courte, en raison d'une obsolescence rapide des données. Selon les éléments disponibles, la durée de conservation des données personnelle en Europe varie de 3 mois à 20 ans, **avec une durée moyenne de 6 ans** (Iron Mountain & De Braw Blackstone Westbroek, 2013). Pour les jeux de données comprenant des données personnelles, les principes de limitation des finalités, de minimisation des données et de limitation de la durée de conservation s'appliquent afin de déterminer la durée pendant laquelle l'ensemble de données peut être utilisé licitement. Par conséquent, **la durée de conservation ainsi déterminée aux fins du RGPD peut constituer une référence pour définir la durée d'amortissement du point de vue comptable.** Cela permet de comprendre pourquoi les jeux de données peuvent être considérés comme des actifs amortissables.

Il est également souvent avancé que le critère de propriété est difficile à satisfaire, en raison de l'existence de droits en matière de protection des données, en particulier les exigences relatives au consentement, qui peuvent limiter la maîtrise économique des bases de données pour les entreprises du numérique. La législation en matière de protection des données permet l'utilisation de données à caractère personnel, y compris dans un contexte commercial, et fournit un cadre permettant de concilier l'utilisation licite des données personnelles, tout en protégeant les droits des personnes en matière de protection des données. Bien que le consentement soit fréquemment invoqué, les entreprises peuvent s'appuyer sur d'autres bases juridiques pour un usage commercial des données. Elles peuvent par exemple collecter des données sur le fondement de l'exécution d'un contrat et les utiliser ensuite sur le fondement de l'intérêt légitime. Le droit à l'effacement est également cité comme un facteur restrictif : il confère aux consommateurs le droit d'obtenir la suppression de leurs données à caractère personnel pour divers motifs. Le RGPD et la loi britannique prévoient toutefois que les entreprises peuvent conserver des données à caractère personnel lorsqu'elles y sont légalement tenues afin de se conformer à des réglementations financières ou autres[21]. À l'inverse, certaines dispositions relatives à la protection des données, telles que le principe d'exactitude des données ou les dispositions permettant à des tiers d'accéder à des données collectées de manière licite, peuvent générer une certaine exclusivité au profit du détenteur des données et renforcer les critères d'identifiabilité et de contrôle prévu par IAS 38. Il apparaît ainsi que, **lorsque le respect des exigences en matière de protection des données est intégré aux processus opérationnels, il peut créer des synergies dans l'application des critères comptables permettant de comptabiliser les données en tant qu'immobilisations incorporelles.**

Évaluation ultérieure et dépréciation au titre d'IAS 36

Une fois comptabilisés, ces actifs, sans préjudice de leur amortissement éventuel, sont soumis à un test de dépréciation conformément à IAS 36 « Dépréciation des actifs », afin de s'assurer qu'ils ne sont pas inscrits au bilan pour une valeur supérieure à leur

21 Your right to get your data deleted | ICO

valeur recouvrable[22].

La valeur recouvrable correspond à la valeur la plus élevée entre la juste valeur d'un actif diminuée des coûts de sortie et sa valeur d'utilité, correspondant à la valeur actualisée des flux de trésorerie futurs attendus de l'actif. À chaque date de clôture, l'entreprise doit déterminer s'il existe des indices indiquant qu'un actif pourrait être déprécié. En outre, le goodwill et les immobilisations incorporelles ayant une durée d'utilité indéterminée ou n'étant pas encore disponibles à l'utilisation doivent faire l'objet d'un test de dépréciation au moins une fois par an.

IAS 36 distingue les indices de dépréciation externes et internes. Dans un contexte fondé sur les données, les indices externes peuvent notamment inclure des évolutions défavorables de l'environnement réglementaire, telles qu'un renforcement des exigences en matière de protection des données. Les indices internes peuvent correspondre à une performance insuffisante d'une base de données client ou à des changements significatifs dans son utilisation.

Lorsqu'un actif ne génère pas de flux de trésorerie indépendantes, le test de dépréciation est réalisé au niveau d'une unité génératrice de trésorerie, définie comme le plus petit groupe identifiable d'actifs générant des entrées de trésorerie largement indépendantes. Cette situation est fréquente dans les environnements pilotés par les données, dans lesquels les bases de données client tirent une valeur de leur intégration avec d'autres actifs.

Si la valeur comptable d'un actif ou d'une unité génératrice de trésorerie est supérieure à sa valeur recouvrable, une perte de valeur est comptabilisée. Cette situation est particulièrement pertinente pour le goodwill, qui intègre souvent des synergies attendues, notamment celles liées à l'utilisation des données. Une détérioration de ces avantages attendus peut donc entraîner une dépréciation[23].

Comparaison avec les normes nationales FR, LU et UK

Le traitement comptable des bases de données clients selon les normes IFRS présente à la fois des similitudes conceptuelles et des différences importantes par rapport aux référentiels comptables français (PCG), luxembourgeois et britanniques (FRS 102).

Dans les différents référentiels comptables, les immobilisations incorporelles sont généralement comptabilisées sur la base de principes sous-jacents similaires, qui exigent leur identifiabilité ainsi que la probabilité de générer des avantages économiques futurs. Alors que les IFRS font explicitement référence au contrôle de la ressource, la norme FRS 102 exige que les avantages économiques futurs attribuables à l'actif soient susceptibles de bénéficier à l'entité et que son coût ou sa valeur puisse être évalué de manière fiable. Ces approches reposent sur un fondement conceptuel commun quant à la nature des immobilisations incorporelles.

Toutefois, les trois référentiels comptables nationaux adoptent une approche plus prudente en matière

22 IAS 36, paragraphes 6, 9 et 10
23 IAS 36, paragraphes 12, 59 et 66.

de comptabilisation des bases de données client générées en interne. Selon ces normes, de tels actifs ne sont généralement pas comptabilisés, car leurs coûts ne peuvent être évalués de manière fiable et ne peuvent être distingués du goodwill généré en interne. En conséquence, les dépenses liées aux fichiers clients développés en interne sont en règle générale, comptabilisées en charges.

Des différences plus significatives apparaissent dans le contexte de regroupements d'entreprises. IFRS 3 impose l'identification systématique et la comptabilisation séparée de toutes les immobilisations incorporelles identifiables, y compris les bases de données clients, même lorsqu'elles n'étaient pas comptabilisées auparavant. En revanche, selon le référentiel français (FR GAAP) et luxembourgeois (GAAP), l'allocation du prix d'acquisition est moins détaillée et les actifs liés à la clientèle sont plus fréquemment inclus dans le goodwill. Le référentiel britannique (UK GAAP) adopte une position intermédiaire : il exige généralement la comptabilisation des immobilisations incorporelles identifiables, mais accorde moins d'importance à une évaluation détaillée que les IFRS.

Des différences sont également observées en matière d'évaluation ultérieure. Selon les normes IFRS, le goodwill n'est pas amorti et fait l'objet d'un test de dépréciation annuel, que selon le référentiel français (FR GAAP), luxembourgeois (LU GAAP) et britannique (UK GAAP), il est généralement amorti sur sa durée de vie utile finie[24]. Cette approche reflète un principe de prudence plus marqué dans les référentiels comptables nationaux, dans lesquels l'amortissement systématique réduit la dépendance à l'égard d'hypothèses d'évaluation prospectives.

Dans l'ensemble, bien que les fondements conceptuels soient globalement alignés, les IFRS adoptent une approche davantage fondée sur des principes et axée sur la réalité économique, notamment en matière de regroupements d'entreprises et de tests de dépréciation, tandis que les référentiels français (FR GAAP) et luxembourgeois (LU GAAP) demeurent plus prudents, et que le référentiel britannique (UK GAAP) se situe dans une position intermédiaire.

La principale différence entre les IFRS et les référentiels comptables nationaux réside dans l'allocation de la valeur des actifs incorporels.

Les IFRS imposent une séparation systématique des immobilisations incorporelles identifiables du goodwill, tandis que les référentiels français et luxembourgeois permettent qu'une part plus importante de la valeur incorporelle, y compris les éléments liés à la clientèle, demeure comprise dans le goodwill.

Le référentiel britannique applique un principe de séparation similaire : il convient de démontrer que les actifs génèrent des avantages futurs et que les coûts engagés sont identifiables pour qu'ils soient comptabilisés en immobilisations incorporelles, tandis que, dans les regroupements d'entreprises, le goodwill est quant à

24 Voir les GAAP français (Plan Comptable Général, articles 214-3 et 214-4) et les GAAP britanniques (FRS 102, section 18.19–18.23), qui exigent que le goodwill soit amorti sur sa durée de vie utile. Les GAAP luxembourgeois suivent une approche prudentielle similaire.

lui comptabilisé en tant qu'actif [25].

Portefeuilles de prêts et traitement comptable des données clients incorporées

Le traitement comptable des portefeuilles de prêts offre un éclairage complémentaire sur la comptabilisation de la valeur incorporelle liée aux clients, en particulier au regard du rôle des données relatives aux emprunteurs. Si les portefeuilles de prêts sont systématiquement comptabilisés en tant qu'actifs financiers dans l'ensemble des référentiels comptables, le traitement des données client qui y sont incorporées révèle des limites conceptuelles importantes.

Dans tous les référentiels comptables, les portefeuilles de prêts sont comptabilisés en tant qu'instruments financiers. Toutefois, les données associées aux emprunteurs, telles que leur comportement en matière de remboursement, leur historique de crédit ou les informations relatives à leur segmentation, ne donnent pas lieu à une comptabilisation séparée en tant qu'immobilisations incorporelles. Cela s'explique principalement par la difficulté de satisfaire aux critères d'identifiabilité et de contrôle. Ces données sont rarement séparables de la relation contractuelle représentée par le prêt lui-même et sont souvent soumises à des contraintes juridiques et réglementaires, notamment en matière de protection des données personnelles.

Selon les IFRS, l'acquisition d'un portefeuille de prêts dans le cadre d'un regroupement d'entreprises peut conduire à l'identification de certains actifs incorporels liés, tels que des droits de gestion ou des accords contractuels, dès lors qu'ils satisfont aux critères de séparabilité ou qu'ils découlent de droits opposables. Dans ce cas, ces éléments sont comptabilisés séparément du goodwill, conformément à l'approche de désagrégation prévue par IFRS 3. En revanche, la valeur plus large associée aux données relatives aux emprunteurs, notamment les informations tirées des données comportementales ou des relations avec les clients, n'est pas comptabilisée en tant qu'actif distinct et demeure soit intégrée à l'actif financier, soit incluse dans le goodwill.

Cette différence porte davantage sur l'importance accordée à ces éléments que sur le principe lui-même dans les référentiels comptables français et luxembourgeois. Bien que la comptabilisation du portefeuille de prêts lui-même reste inchangée, il n'est pas obligatoire d'identifier et de séparer systématiquement, dans le cadre d'un regroupement d'entreprises, les éléments incorporels liés aux données. Par conséquent, une part plus importante de la valeur économique sous-jacente, y compris celle associée aux données client, reste incluse dans le goodwill ou est implicitement prise en compte dans l'évaluation de l'instrument financier.

Le référentiel britannique (UK GAAP) suit une approche conceptuelle proche des IFRS en exigeant l'identification des immobilisations incorporelles lorsqu'elles sont séparables ou contractuelles. En pratique, toutefois, un nombre plus limité d'éléments est comptabilisé séparément, ce qui conduit, à l'instar des référentiels français et luxembourgeois, à une concentration plus forte de la valeur au sein du goodwill.

Dans l'ensemble, si les portefeuilles de prêts sont comptabilisés de manière homogène dans les différents référentiels, la valeur économique tirée des données relatives aux emprunteurs n'est que partiellement reflétée dans les états financiers. Comme pour les bases de données client, **la distinction essentielle ne tient pas à l'existence de l'actif, mais à la mesure dans laquelle ses composantes sous-jacentes sont identifiées séparément ou absorbées dans le goodwill.**

25 Selon les GAAP britanniques (FRS 102, sections 18 et 19), les actifs incorporels identifiables sont comptabilisés séparément du goodwill dans un regroupement d'entreprises s'ils répondent aux critères de définition et de comptabilisation. Ils sont évalués à la juste valeur à la date d'acquisition, mais la norme n'exige pas le même niveau d'identification et d'évaluation détaillées qu'IFRS 3, ce qui peut entraîner une diminution des actifs incorporels comptabilisés séparément

Catégorie	Exemples	Génération de données ?	Comptabilisé	Non comptabilisé	Norme IFRS
Basé sur la technologie	Logiciels, plateformes, coûts de développement	Oui	Logiciel acquis ou développé en interne (phase de développement uniquement)	Phase de recherche, données brutes générées en interne	IAS 38
Lié aux clients	Fichiers clients, relations	Très élevé	Fichiers clients acquis (par exemple lors de fusion-acquisition)	Fichiers clients générés en interne	IAS 38 / IFRS 3
Lié au Marketing	Marques, marques déposées	Oui	Marques et marques déposées acquises	Marques générées en interne	IAS 38
Propriété intellectuelle	Brevets, droits d'auteur, droits de PI attachés à des bases de données	Oui	Droits de propriété intellectuelle juridiquement établis (brevets, droits d'auteur et bases de données), droits de PI attachés aux bases de données	Savoir-faire non protégé	IAS 38
Basé sur un contrat	Licences, franchises, accords	Oui	Droits contractuels (licences, accords)	Contrats indissociables	IAS 38
Savoir-faire	Procédés, secrets d'affaires	Oui	Si identifiable et légalement protégé	Savoir-faire diffus/ interne	IAS 38
Données (actif autonome)	Jeux de données internes, données brutes	Central	Données acquises à l'extérieur, jeux de données spécialisés	Données brutes générées en interne	IAS 38
Goodwill et données incorporées	Goodwill (y compris la valeur des données)	Indirect	Comptabilisé lors des regroupements d'entreprises	Goodwill généré en interne	IFRS 3 / IAS 38

Tableau 1 – Comptabilisation et répartition des bases de données clients selon les normes IFRS et les dans référentiels nationaux

3.3 Incidences de la conformité à la protection des données sur les transactions et sur l'évaluation financière

Les pratiques comptables jouent un rôle important dans la manière dont les organisations évaluent et comptabilisent la valeur des actifs liés aux données. Cependant, la valeur des données et les avantages tirés de la conformité ne se limitent pas aux seules considérations comptables.

Dans de nombreux cas, **l'évaluation intervient en dehors du cadre comptable, en particulier dans le contexte de transactions portant sur la valeur économique d'une entreprise,** par opposition à sa valeur comptable. Ainsi, dans les opérations de gré à gré, notamment dans le cadre de fusions-acquisitions, en vue d'une introduction en bourse (IPO) ou lors d'opérations de financement, la valeur comptable apparait généralement limitée et doit être complétée par d'autres éléments afin de mesurer pleinement la création de valeur générée par l'entreprise. Lors d'opérations de gré à gré, lorsqu'aucun prix de marché n'a pas encore été établi, les investisseurs tendent généralement à valoriser la transparence et la solidité des dispositifs de gouvernance des données, tandis que des politiques de gestion des données insuffisantes sont souvent pénalisées.

Dans ce type de contexte, **la valeur des données et le respect des exigences réglementaires prennent toute leur importance, car ils peuvent exercer une influence significative sur l'évaluation des transactions. Cela est particulièrement vrai dans l'économie numérique et pour les acteurs technologiques.** Toutefois, avec la numérisation croissante de l'économie, les pratiques en matière de données finissent par concerner un large éventail de secteurs, tant dans le commerce de détail que dans les activités interentreprises (B2B). Selon une étude réalisée par EY, en 2024, les actifs incorporels (comptabilisés ou non) et le goodwill représentaient 79 % de la capitalisation boursière du CAC 40 (EY, 2025). Une partie de cette valeur repose sur les actifs de données. Au Royaume-Uni, en 2023, l'ensemble des entreprises a investi 244,7 Mds de livres dans des actifs incorporels, soit 85,3 Mds de livres de plus que dans les actifs corporels (ONS, 2025). Les investissements dans les actifs incorporels sont supérieurs à ceux dans les actifs corporels depuis 1998, l'écart ne cessant de se creuser (ibid.). De même, au Luxembourg, les investissements dans les actifs incorporels ont représenté 15 % de la valeur ajoutée brute (VAB) en 2019, contre 11 % pour les investissements dans les actifs corporels (Conseil national de la productivité, 2023).

De plus, les opérations de gré à gré prennent de plus en plus en compte la valeur des données du point de vue comptable, comme indiqué dans la sous-section précédente, et reflètent ainsi l'évolution de la réalité financière intégrant la valeur des données.

Dans cette perspective, l'approche retenue dans le présent rapport est double. **L'intégration des aspects liés aux données dans les évaluations financières ne peut pas reposer uniquement sur les risques liés aux données,** c'est-à-dire le risque de pertes de valeur lorsque les données sont mal gérées ou lorsque les exigences de conformité ne sont pas correctement respectées. **Elle doit également prendre en compte les opportunités de création de valeur découlant des actifs liés aux données eux-mêmes**, ainsi que les avantages associés à une bonne gouvernance et au respect des exigences de conformité. **Ces deux dimensions sont indissociables :** ce n'est que lorsque la valeur des données est clairement évaluée que les risques peuvent être quantifiés, et inversement, une bonne connaissance des actifs liés aux de données permet d'identifier les risques de manière pertinente. **Pour cette raison, toute évaluation de la valeur des données et de l'impact économique du respect des exigences conformité devrait tenir compte à la fois des avantages et des risques potentiels**. Cet équilibre a été confirmé par les praticiens ayant participé à l'atelier Daprolab[26] et est également reconnu dans l'enquête Deloitte Tech Value de 2025, qui constate que l'évaluation des données et la « dette liée aux données » (« data debt ») sont intrinsèquement liées dans les décisions d'investissement (Deloitte, 2025)[27].

3.3.1 Enseignements tirés des sources publiques et des entretiens

L'idée selon laquelle la valeur des données est souvent sous-estimée ou insuffisamment prise en compte par les référentiels existants, par rapport à leur valeur économique pour l'entreprise, n'est pas nouvelle et est même largement présente dans la littérature économique. Au cours ces deux dernières années, l'OCDE[28] a élaboré un cadre visant à intégrer la valeur des données en tant qu'actif dans dans les référentiels de comptabilité nationale (OCDE, 2022). Cette approche considère les données, **d'un point de vue macroéconomique, comme un investissement. Selon l'OCDE,** le « capital de données » représente entre 5 % et 9 % du PIB en Europe (OCDE, 2022, p. 29)[29]. S'agissant du traitement comptable des données, cette étude conclut clairement que « la valeur des données et des actifs incorporels dans les données au niveau des entreprises est sous-estimée » (Ibid. p17)[30]. Comme indiqué dans la section consacrée à la revue de la littérature, la littérature économique a cherché à combler cet écart. Plusieurs approches coexistent, le sujet étant encore relativement récent, et certains rapports ont recommandé aux pouvoirs publics de développer des méthodes d'évaluation des données en tant que telles (Frontier Economics, 2021). Des chercheurs ont publié un modèle d'évaluation des données fondé sur l'approche des flux de trésorerie actualisés (Discounted Cash Flow, DCF) (Cheong et al., 2023). D'autres ont concentré leurs travaux, là encore dans le cadre d'un article publié, sur d'entreprises technologiques cotées en bourse, sur la base de métriques de marché (Xiaochuan, et al., 2026). En ce qui concerne la disponibilité de services d'évaluation, les entretiens réalisés ont mis en évidence

26 Cet atelier a eu lieu en juillet 2026 à la CNPD de Luxembourg.

27 La dette liée aux données résulte de facteurs tels que les coûts associés à leur cycle de vie, les problèmes de qualité, les risques en matière de conformité et de sécurité des données, ainsi que l'obsolescence des données, qui contribuent à en réduire la valeur.

28 Voir https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/11/measuring-data-as-an-asset_cf2c5025/b840fb01-en.pdf

29 Selon les entretiens réalisés avec les parties prenantes.

30 Selon les entretiens réalisés avec les parties prenantes.

l'émergence de différents cabinets de conseil qui se spécialisent désormais dans l'évaluation économique des actifs liés aux données à des fins financières.

Les recherches publiées montrent également qu'une plus grande transparence des entreprises procédant à une introduction en bourse (IPO) concernant leurs politiques et leurs risques entraîne une réduction des asymétries d'information, ce qui conduit les investisseurs à atténuer leurs pratiques de sous-tarification (Ding, 2016). Ce phénomène peut s'expliquer d'un point de vue microéconomique : en l'absence d'informations suffisantes entre les parties, les transactions de marché peuvent conduire à des résultats sous-optimaux, ce qui réduit l'efficacité du fonctionnement des marchés.

Dans cette perspective, il apparaît clairement pourquoi et comment la conformité et la gouvernance des données jouent un rôle essentiel dans la préservation de la valeur de ces actifs. Les entretiens réalisés dans le cadre de cette étude ont notamment montré, et l'un des participants l'a souligné, que « **la conformité protège la valeur en garantissant que les données peuvent générer légalement et durablement des flux de trésorerie futurs** »[31]. Des professionnels des fusions-acquisitions ont indiqué que « dans les opérations de fusion-acquisition, la licéité et la gouvernance des données influencent directement l'évaluation, la structure de la transaction et la capacité à finaliser une opération ». D'autres ont souligné que « **des pratiques solides en matière de protection des données préservent la valeur de la transaction et réduisent le risque lié à l'opération** » dans le cadre des opérations financières.

3.3.2 Conformité des données et risques dans les notations de crédit

Un exemple notable de cette évolution concerne l'impact des violations de données sur les notations des entreprises. Pendant longtemps, la protection des données et la cybersécurité ont été traitées comme des enjeux essentiellement techniques ou juridiques. Toutefois, une série d'incidents (par exemple l'affaire Yahoo en 2013) ayant eu des répercussions visibles sur les bilans des entreprises, a modifié la manière dont les agences de notation appréhendent ces questions. Celles-ci intègrent désormais le risque cyber, les pratiques en matière de protection des données, ainsi que les dispositifs de gouvernance et de gestion des risques associés dans leur évaluation du profil de risque d'une organisation. Les agences de notation évaluent la capacité de crédit d'une organisation, c'est-à-dire sa capacité à assurer le service de sa dette. Leur analyse du risque lié aux « données » s'inscrit donc dans une perspective d'évaluation de solvabilité, plutôt que dans une logique d'évaluation de la valeur de l'entreprise. La protection des données n'est pas considérée comme une catégorie à part entière, elle est intégrée à l'analyse de la cybersécurité, de la « posture cyber », de l'exposition aux risques et de leur gouvernance.

Alors que l'impact d'une violation de données sur le cours de l'action est souvent volatil et de courte durée, **une agence de notation est susceptible d'avoir un effet plus durable notamment par l'intermédiaire du marché obligataire.** A long terme, ni les notations ni les cours des actions ne sont durablement affectés. L'effet documenté des violations de données est principalement de court terme, compte tenu du caractère « non continu » de l'événement.

Les agences de notation peuvent intervenir à deux niveaux : en révisant la perspective (une perspective négative signale une probabilité accrue d'une future dégradation de la notation) ou en abaissant directement la notation (dégradation). Le mécanisme financier permettant d'évaluer l'incidence des violations de données ou des incidents cyber affectant les notations est le suivant : une dégradation de la notation accroît le risque de défaut perçu de l'émetteur, de sorte que les investisseurs exigent un spread de crédit plus élevé (c'est-à-dire la prime payée au-dessus du taux sans risque) lors de nouvelles émissions. Mécaniquement, un spread plus élevé se traduit par un coupon plus élevé et, par conséquent, par un coût de financement à long terme plus important. Le coût d'une dégradation n'est pas linéaire et varie en fonction des conditions du marché. Il demeure généralement modéré au sein de la catégorie investment grade, mais augmente fortement à l'approche de la frontière BBB- et BB+. Pour les émetteurs dits à haut rendement ou high yield, l'effet est généralement plus important, les pertes liées aux incidents cyber venant renforcer la fragilité de ces entités. **La valeur ajoutée de ce processus réside dans l'accès à des informations non publiques et spécifiques à l'entreprise**, y compris des données obtenues directement auprès de la direction, permettant une évaluation plus éclairée du profil de risque et de la résilience de l'entité.

Les notations peuvent avoir une incidence sur deux domaines. Le premier concerne la capacité du résultat avant intérêts, impôts, dépréciation et amortissement (EBITDA) à couvrir les charges, principalement déterminée à partir des flux de trésorerie futurs et de l'analyse du bilan. Le second concerne les informations que la notation fournit implicitement sur le profil de risque d'une entreprise, y compris ses avantages concurrentiels et sa position sur le marché. En pratique, les agences de notation prennent des mesures négatives à l'égard d'une notation lorsqu'une attaque perturbe significativement les activités essentielles de l'entreprise et entraîne des conséquences financières à plus long terme. Nos entretiens ont montré que l'incidence sur la solvabilité était évaluée à partir de plusieurs questions, notamment le degré de perturbation des activités essentielles de l'entreprise, l'efficacité de la gestion visant à contenir les dommages, l'impact sur les indicateurs de crédit, les pertes absorbées, ainsi que les antécédents de l'entreprise en matière d'incidents. **L'évaluation repose fondamentalement une analyse exclusivement orientée à la baisse.** Un incident semble pénaliser l'émetteur, tandis que l'amélioration des pratiques en matière de données ne semble générer aucun effet positif sur les notations.

Si l'intérêt d'une telle pratique réside dans la prise en compte de l'exposition des données et les risques qui y sont associés, les limites de cette approche peuvent être comprises au regard des pratiques de marché (voir section 3.1), qui ne permettent pas toujours de quantifier les efforts déployés en matière de conformité aux exigences relatives aux données ou de bonne gouvernance. À l'inverse, certains aspects liés à la conformité en matière de protection des données pourraient être pris en compte positivement dans les notations des entreprises,

31 Selon les entretiens réalisés avec les parties prenantes.

notamment au travers de l'évaluation des stratégies ESG. Toutefois, ces approches ne semblent pas encore suffisamment matures pour intégrer de manière systématique le respect des exigences en matière de protection des données, comme cela a été examiné dans la section du rapport consacrée à la gouvernance organisationnelle.

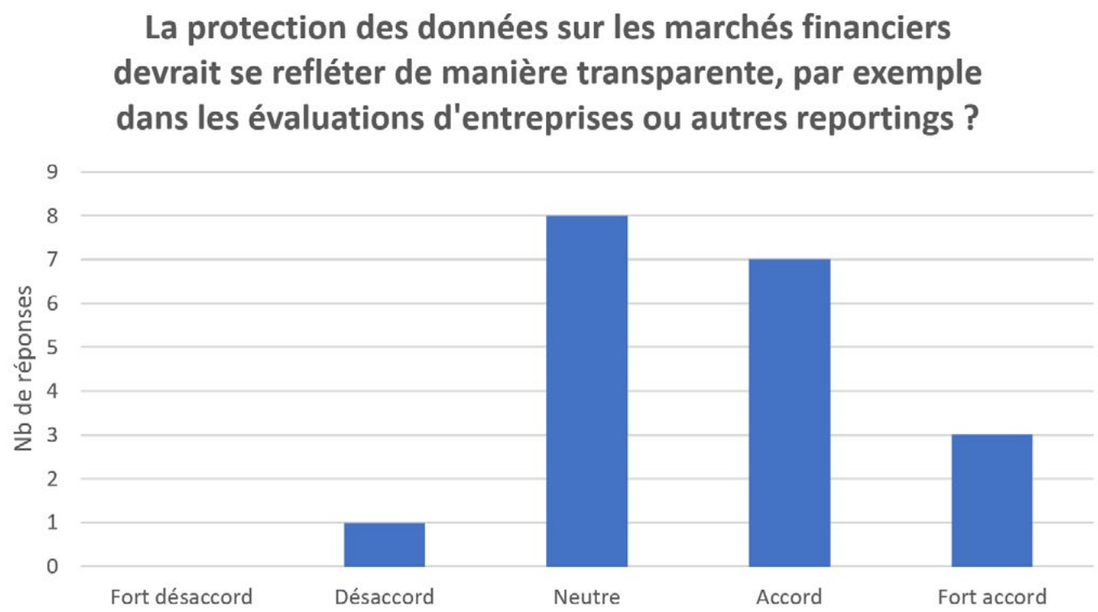
Comme nous l'avons déjà vu à la section 3.1, les marchés boursiers ne quantifient généralement pas le respect de la réglementation, dans la mesure où les entreprises sont supposées se conformer aux exigences réglementaires. Cela conduit à l'application de facteurs de pénalisation lorsque des informations publiques révèlent que tel n'est pas le cas, par exemple lorsqu'un manquement est signalé par une autorité de régulation ou mis en évidence à la suite d'une violation de données. Toutefois, **cette approche ne permet pas de démontrer suffisamment l'importance des enjeux liés à la protection des données pour l'écosystème financier.** Pour une entreprise, le nombre de réclamations reçues ou la gravité des violations de données subies reflète la qualité de sa « gestion responsable des données » (data stewardship) et de sa politique de protection contre les cybermenaces. Plus cette qualité est faible, plus les risques susceptibles d'affecter la réputation de l'entreprise sont probables et coûteux ; à l'inverse, plus cette qualité est élevée, plus le niveau de confiance des clients, des partenaires commerciaux et des agences de notation est important.

La transparence des pratiques de protection des données permet aux marchés d'apprécier les activités des entreprises dans leur ensemble et non seulement de les pénaliser en raison de leur exposition aux risques, de reconnaître les efforts qu'elles déploient en faveur de pratiques conformes en matière de données.

3.3.3 Résultats de l'enquête quantitative

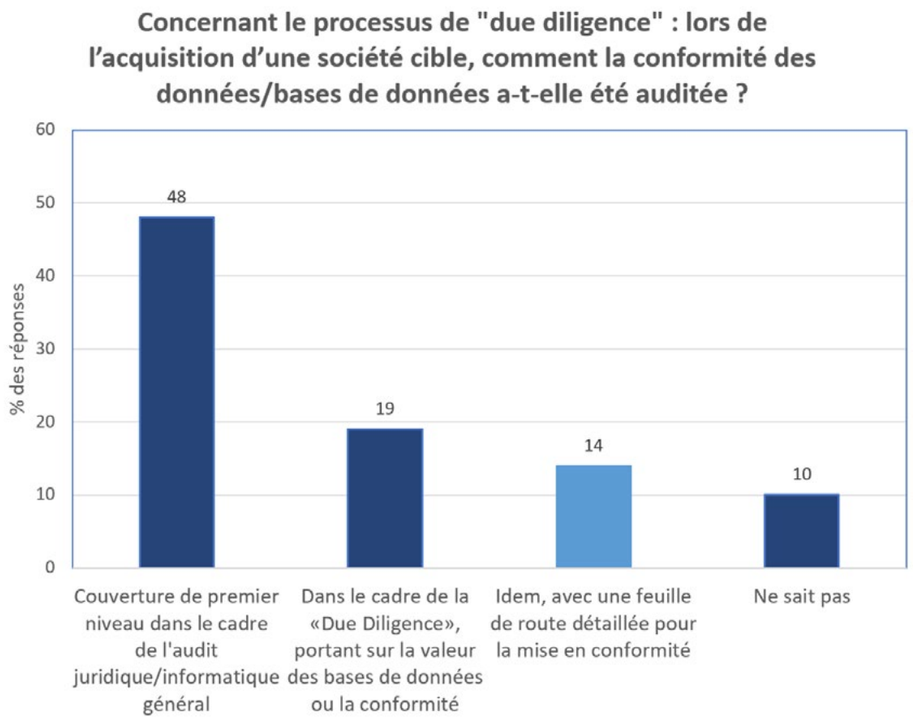
Les éléments quantitatifs recueillis dans le cadre de cette étude plaident en faveur de l'intégration des informations relatives à la protection des données dans l'évaluation des opérations de fusions-acquisitions. L'enquête a été menée par la CNIL auprès de DPO français. Parmi 204 répondants, 37 % avaient réalisé une opération de fusion-acquisition au cours des cinq dernières années.

Invitées à indiquer, sur une échelle de 1 à 5, si « la protection des données devrait être reflétée de manière transparente, par exemple dans l'évaluation des entreprises ou dans d'autres rapports financiers », les entreprises ayant réalisé des opérations de fusion-acquisition au cours des cinq dernières années ont attribué une note moyenne de 3,63, **donc plutôt favorable à cette affirmation** (voir Graphique 1 ci-dessous), et une seule entreprise a exprimé son désaccord avec ce point de vue.



Graphique 1 : enquête auprès des entreprises françaises ayant réalisé une opération de fusion-acquisition au cours des 5 dernières années, mai 2026.

Les éléments recueillis suggèrent que les opérations de fusions et acquisitions constituent un levier favorisant la prise en compte et la communication de la valeur financière des données. Cela n'est pas surprenant, dans la mesure où ces transactions reposent sur l'évaluation financière des entreprises, et non uniquement sur leur valeur comptable ou leur valeur de marché. Les éléments recueillis indiquent la conformité en matière de données constitue l'un des indicateurs pris en compte dans les opérations de fusion-acquisition, bien que, dans la majorité des cas, elle le soit de manière assez générale. **Toutefois, dans certains secteurs où les données jouent un rôle particulièrement important, les procédures de due diligence peuvent aller plus loin et prendre en compte, de manière plus spécifique, la valeur des bases de données ainsi que le niveau de conformité de l'entreprise** en matière de protection des données (voir Graphique 2). Dans 14 % des cas, **ces procédures intègrent même une feuille de route précisant les mesures à mettre en œuvre pour assurer ou renforcer la conformité.**



Graphique 2 : enquête auprès entreprises françaises ayant participé à une opération de fusion-acquisition au cours des 5 dernières années, mai 2026.

Cela étant, l'évaluation financière des risques liés aux données ne constitue pas encore une pratique généralisée et, si les opérations de fusion-acquisition jouent un rôle d'accélérateur, l'évaluation de ces risques ne semble pas encore être intégrée de manière systématique dans les processus de décision des entreprises. Les entreprises ayant réalisé des opérations de fusion-acquisition au cours des cinq dernières années sont davantage susceptibles d'intégrer les risques liés aux données dans les notations de crédit ou dans leurs bilans (voir Tableau 2). Néanmoins, **le potentiel d'intégration de la valeur associée à la conformité en matière de protection des données dans les transactions financières demeure important.** L'ambition de ce rapport est de mettre en évidence les bonnes pratiques en la matière et, nous l'espérons, de contribuer à leur développement.

	Répondants n'ayant pas participé à un opération de fusion-acquisition	Répondants ayant participé à une opération de fusion-acquisition
Dans une acquisition passée	4,5%	13,5%
Dans la notation de crédit	3%	6%
Au bilan ou dans la méthode DCF	3%	6%
Total	10,5%	25,5%

Tableau 2 : Réponses à la question « À votre connaissance, comment les risques liés aux données sont-ils principalement pris en compte dans l'évaluation financière de votre entreprise, que ce soit en interne ou via des acteurs externes ? », répondants DPO français, mai 2026[32].

32 Les différences sont statistiquement significatives avec une valeur p-value de 0,024 et de 0,035 après contrôle pour la taille de l'entreprise.

3.3.4 Aspects transactionnels (fusions et acquisitions) et considérations relatives à la due diligence

Les transactions financières (dans le cadre d'introductions en bourse (IPO), d'opérations de fusion-acquisition ou de financements) permettent de dépasser le dilemme relatif à la communication d'informations sur les données dans le cadre de la due diligence, évoqué précédemment. Dans de tels cas, les émetteurs d'instruments financiers tels que les actions **communiquent les informations relatives aux données et à la conformité à un nombre restreint de contreparties potentielles, qui réalisent le processus dit de « due diligence ».** Celui-ci conduit l'émetteur ou la société cible à communiquer des informations propres à l'entreprise à un acquéreur ou à un investisseur, ou à leurs conseils. Il est indéniable que de tels processus revêtent une importance majeure dans l'économie numérique actuelle, voire dans l'économie dans son ensemble, et en particulier dans les secteurs les plus innovants. Selon les données de PWC, la capitalisation cumulée des 100 premières entreprises mondiales s'élevait à 51 800 milliards de dollars au début de 2026, tandis que le montant des opérations de fusion-acquisition atteignait 4 500 milliards de dollars en 2025, soit une hausse de 50 % par rapport à 2024 (PWC, 2026). Dans ce contexte, les sociétés de capital-risque détenaient 3 500 milliards de dollars d'actifs sous gestion dans le monde, selon le World Economic Forum, ces investissements concernant souvent des entreprises exposées à des risques importants liés aux données.

L'activité de fusion-acquisition est plus importante dans les entreprises fortement dépendantes des données (Schoch, 2020), ce qui reflète le phénomène qualifié de « data-driven mergers », dans lequel de grands acteurs acquièrent directement les entreprises plutôt que leurs ensembles de données, afin d'éviter les contraintes juridiques liées à la protection des données. Ce phénomène est encore plus marqué avec l'essor de l'intelligence artificielle générative, dans lequel les ensembles de données utilisés pour l'entraînement des modèles sont devenus une composante stratégique de l'innovation économique et présentent une structure susceptible de faciliter le respect des critères comptables permettant leur comptabilisation en tant que bases de données spécialisées, comme indiqué à la section 3.2.

Dans le processus de fusion-acquisition, la licéité des bases de données a clairement un impact sur leur utilisation et leurs rendements futurs. Selon la jurisprudence des juridictions françaises, un fichier non conforme ne peut être légalement cédé : il n'a pas de valeur économique et la clause prévoyant sa cession est illicite [33]. De la même manière, le volume et la qualité des jeux de données influent sur les revenus futurs de la cible et, partant, sur le prix de la transaction. Enfin, du point de vue des risques, des pratiques insuffisantes en matière de gestion et de gouvernance des données entraînent des demandes d'exercice des droits plus nombreuses et des coûts plus élevés pour les entreprises. Le même raisonnement vaut pour les cessions d'actifs (où seuls des actifs incorporels comportant une composante « données » sont cédés) et pour les cessions de titres (où sont cédées les actions d'une entreprise de données, par exemple dans le cadre d'un investissement en capital-risque).

Comment réduire les asymétries d'information liées aux données lors de la préparation d'une opération de fusion-acquisition, en intégrant ces informations dans le processus de due diligence ?

Le graphique suivant illustre le processus de due diligence dans les opérations de fusion-acquisition. L'ensemble du processus peut durer de 6 à 18 mois. Il peut être également être adapté aux opérations de financement et aux introductions en bourse (IPO).

Le processus débute par la diffusion d'un mémorandum d'information public, auquel un ou plusieurs acquéreurs potentiels peuvent répondre, et s'accorder sur un accord de confidentialité (Non-Disclosure Agreement, NDA) contractuellement contraignant. La phase de due diligence est menée avec chacun de ces acquéreurs potentiels, sur la base d'une « data room » contenant les informations pertinentes, d'échanges de questionnaires écrits et de réunions avec la direction de la société cible. Lorsque la société cible sélectionne l'un des acquéreurs potentiels, les négociations deviennent exclusives et l'acquéreur approfondit ses travaux de due diligence afin d'obtenir des informations supplémentaires. La signature de la transaction stabilise les conditions de l'opération, mais le contrat ne devient juridiquement contraignant qu'au moment de la réalisation de l'opération. Enfin, les modalités de l'opérations peuvent être précisées et complétées après la transaction, par exemple au moyen d'un contrat de services transitoires (Transitional services agreement, TSA).

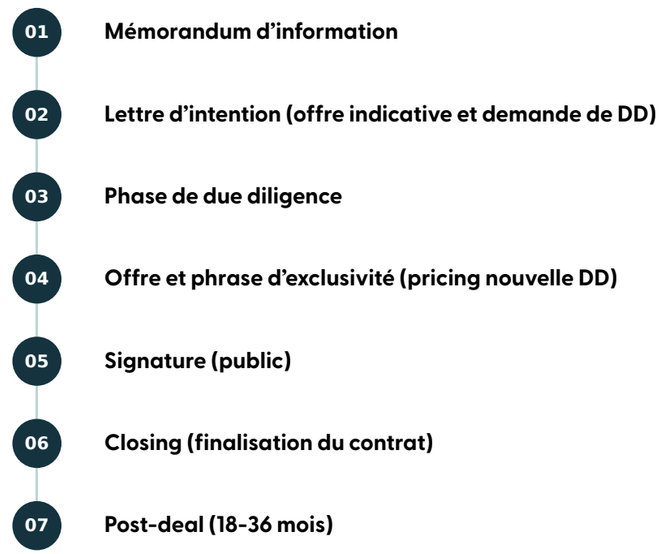


Fig. 1 : les phases du processus de fusion et acquisition, adapté de Ceddaha, 2025.

Les aspects relatifs aux données, tant en ce qui concerne les opportunités que les risques, sont actuellement pris en compte ou peuvent l'être, voire évoluer vers une véritable Data Due Diligence (DDD), en fonction de l'entreprise, de son modèle économique et de ses risques. Ils sont principalement examinés au cours de la phase intermédiaire du processus (due diligence et phase d'exclusivité). Ils peuvent également être pris en compte après la réalisation de la transaction, au moyen d'une feuille de route de conformité des données (voir ci-dessous), par exemple lors de la mise en œuvre des aspects opérationnels de la gestion des données. Les professionnels insistent toutefois sur l'examen des enjeux liés aux données le plus tôt possible, afin qu'ils puissent éclairer les choix de recherche tant de la cible que des acquéreurs. Les opportunités

33 Cour de cassation, chambre commerciale, 25 juin 2013.

peuvent être présentées par la société cible dès le stade du mémorandum d'information, tandis que la lettre d'intention peut souligner l'intérêt d'accorder une attention particulière aux risques liés aux données dès la phase de due diligence.

En ce qui concerne le processus de due diligence proprement dit (phases en gris sur la figure 1), il est devenu plus complexe et plus diversifié au fil du temps, en particulier pour les parties ayant une connaissance plus limitée du processus de fusion-acquisition. **Il couvre les aspects informatiques et ESG ainsi que la conformité réglementaire (aspects juridiques). La protection des données se situe à l'intersection de ces différentes questions** et il n'existe pas d'avantage évident quant à son rattachement à l'une ou l'autre de ces composantes. En matière de protection des données, ni les aspects juridiques ni les aspects techniques ne doivent être sous-estimés. Plus haut, nous avons identifié des indicateurs tel que le reporting ESG, les indicateurs clés de performance (KPI) relatifs à la conformité en matière de protection des données destinés au Conseil d'administration, ainsi que la quantification de la valeur de la protection des données dans les états financiers, qui pourraient être utilisés pour démontrer la conformité d'une entreprise en matière de protection des données dans le cadre de la due diligence. **Une approche globale consisterait également à créer une due diligence spécifique en matière de protection des données (DDD), dotée d'une forte composante d'évaluation et s'appuyant sur des conseils financiers spécialisés.** Cette approche permettrait d'intégrer efficacement les considérations juridiques et techniques dans l'évaluation financière, en prenant en compte à la fois les bénéfices d'une bonne gestion des données et du respect des règles en matière de protection des données, et les risques découlant de contrôles insuffisants, d'une supervision défaillante ou d'incidents liés aux données.

Le plus souvent, la due diligence repose sur un premier niveau d'examen de l'audit juridique ou de l'audit informatique (cf. graphique 1). Cette approche se traduit principalement par une déclaration générale de conformité de la part de l'entreprise cible, qui, par construction, ne peut pas faire l'objet d'un audit et est peu susceptible de permettre une identification adéquate des risques et des opportunités pour l'activité. Ce type d'approche consistant à « cocher les cases » constitue une pratique sous-optimale tant pour l'entreprise acquéreuse que pour l'entreprise cible, car elle ne permet pas de réduire les asymétries d'information existantes.

Les éléments recueillis au cours de cette étude, ainsi que la revue de littérature, indiquent que **le processus de due diligence gagnerait à adopter une approche plus granulaire**, fondée sur une matrice d'audit présentée dans la figure 2.

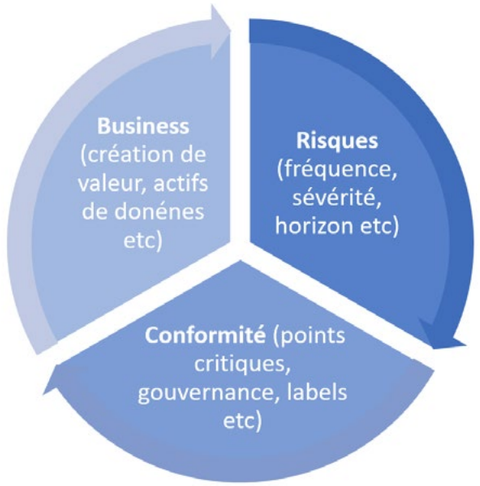


Fig. 2 : Proposition de matrice d'audit simplifiée pour une Data Due Diligence dotée d'une matérialité financière.

Première étape de la due diligence data

Une due diligence data devrait comporter :

- Une description de **la manière dont les données et la conformité en matière de données ont une influence sur les modèles économiques et la création de valeur** de l'entreprise, ainsi que sur ses produits ou les services et une évaluation des données détenues par l'entreprise, de leur volume, de leur qualité et de leur degré de structuration ;

- Une liste des risques liés aux données détenues par l'entreprise, de leur probabilité, de leur gravité et de leur horizon temporel, en commençant par la sensibilité des données, ainsi que des techniques d'atténuation possibles, accompagnée d'une évaluation des rôles des différentes parties prenantes (par exemple les clients, les partenaires commerciaux, les autorités de régulation et les attaquants) ;

- **Une évaluation simplifiée de la conformité de l'entreprise** en matière de protection des données, ainsi qu'une évaluation du niveau de maturité de ses dispositifs de gouvernance, de ses contrôles et de ses pratiques de gestion des données, de même que de l'existence de certifications et de mécanismes d'assurance reconnus susceptibles de contribuer à la création de valeur. Il peut notamment s'agir de certifications en matière de protection des données, de l'adhésion à des codes de conduite ou encore d'une certification selon des normes telles que l'ISO/IEC 27001.

En outre, lorsque cela est pertinent, les acquéreurs potentiels pourraient disposer d'un rapport de due diligence vendeur (Vendor Due Diligence – VDD), présentant la valeur générée par les actifs de données de l'organisation et les capacités métier qui leur sont

associées. Le rapport pourrait également présenter le dispositif de gouvernance de l'organisation, ses mécanismes de conformité et ses processus de gestion des données, contribuant ainsi à démontrer la valeur des investissements antérieurs dans la gestion des risques, la protection des données et les contrôles opérationnels. L'acquéreur procéderait ensuite à sa propre évaluation des risques résiduels et des problèmes de conformité significatifs.

Deuxième étape de la due diligence data

Une fois cette étape achevée, les parties à la transaction évalueraient les informations relatives aux données révélées par le processus de due diligence, ainsi que leur incidence sur le prix et les conditions de la transaction de fusion-acquisition.

Si le processus de due diligence révèle la nécessité d'apporter des changements urgents en matière de conformité ou de prendre des mesures urgentes de réduction des risques, **ces changements peuvent être intégrés dans des clauses suspensives** (covenants) entre les étapes de signature et de closing. Cette approche n'est peut-être pas la plus efficace pour des changements majeurs, car la période entre la signature et le closing est susceptible de durer quelques semaines ou quelques mois. Une incitation plus efficace pour l'entreprise cible pourrait consister à **négocier des compléments de prix (« earn-out »),** c'est-à-dire un supplément de prix versé si certaines conditions sont remplies, au moment du closing ou même après celui-ci. Ce mécanisme peut par exemple permettre de financer les dépenses d'investissement (capex) requises par de nouvelles mesures de mise en conformité ou de réduction des risques, sans avoir d'incidence négative sur le prix de l'opération.

Plus fondamentalement, l'objectif d'une DDD appropriée devrait être de **réduire la probabilité de mise en jeu de la garantie de passif ou d'actif net et par conséquent d'en réduire le coût,** lorsqu'une telle garantie est prévue. Le contrat d'acquisition part en effet du principe que l'entreprise est en conformité avec la réglementation : il est dans l'intérêt de l'entreprise cible de documenter cette conformité, puisque le risque restera à la charge de l'entreprise pendant un certain temps. Cela est d'autant plus vrai dans le cas d'une acquisition de titres, où le risque est supporté par l'entreprise. La garantie de passif peut également être mise en jeu si un risque non identifié se réalise. Des acteurs externes, tels que des assureurs spécialisés, peuvent évaluer le coût de ces risques, ce qui peut conduire à une augmentation du prix de la transaction si ces risques sont correctement identifiés et atténués, notamment grâce à une réduction du coût de la garantie.

Troisième étape : feuille de route « données et conformité »

Enfin, la bonne pratique la plus importante identifiée lors de nos entretiens (et confirmée par les résultats de l'enquête quantitative) est la définition d'une feuille de route « données et conformité » pour la phase post- transaction.

Une gouvernance solide, une bonne gestion des données et une conformité rigoureuse peuvent en effet constituer non seulement un levier de création de valeur pendant l'opération de fusion, mais également contribuer à améliorer la gouvernance, les systèmes informatiques et les pratiques de gestion des données tant de l'entreprise cible que de l'acquéreur. Les bénéfices qui en résultent pour l'entreprise cible peuvent parfois être supérieurs à ceux de l'acquéreur, permettant ainsi à ce dernier de bénéficier d'opportunités inattendues au cours de la phase post-transaction. Au-delà de cet alignement sur les bonnes pratiques, une fusion ou l'entrée d'un nouvel actionnaire au capital peut conduire à revoir les processus opérationnels d'une entreprise, qui pourraient bénéficier directement d'amélioration en matière de conformité à la réglementation sur la protection des données.

Une feuille de route « Données et Conformité » pluriannuelle permet également de réduire le coût de la garantie de passif, voire de la rendre obsolète, en optimisant le profil des données de l'entreprise cible. **Les nouveaux investissements (capex), s'ils sont requis par la feuille de route, peuvent être financés par une série de compléments de prix conditionnés à la réalisation de la feuille de route ; ceux-ci peuvent à leur tour être financés par les réductions correspondantes des coûts opérationnels de l'acquéreur.**

En conséquence, les risques seraient identifiés et atténués, et le prix de la transaction refléterait davantage la valeur globale de l'entreprise et ne serait pas affecté par les asymétries d'information. **Toutes choses égales par ailleurs, le prix de l'opération serait vraisemblablement plus élevé** et/ou pourrait justifier des multiples[34] plus élevés lorsqu'il s'agit de quantifier la création de valeur. En outre, **les négociations de fusion-acquisition pourraient être plus prévisibles, plus équilibrées et, au final, avoir davantage de chances d'aboutir.**

3.3.5 Aspects d'évaluation financière

Nous avons examiné les avantages liés à l'intégration de l'évaluation des actifs de données et des risques associés dans les notations de crédit et les opérations de fusion-acquisition. Dans cette section, nous abordons d'autres aspects des transactions financières qui pourraient bénéficier de la prise en compte de ces actifs et risques liés aux données.

Dans une économie numérisée, où les actifs incorporels sont imparfaitement reflétés par les référentiels et indicateurs actuellement en vigueur, la prise en compte de la valeur des données contribue à expliquer l'existence de multiples importants dans les évaluations financières (généralement entre 5 et 25 selon le secteur [35]). L'intégration des actifs liés aux données et de la conformité en matière de données dans les évaluations financières améliore l'efficience de la détermination du coût du capital des entreprises. Cette approche a été mise en évidence par les enseignements tirés des entretiens réalisés dans le cadre de l'étude et est

34 Les multiples financiers, ou price-to-book ratios, sont des outils permettant d'évaluer la valeur financière d'une entreprise en se basant sur le rapport entre sa valeur de marché et un indicateur comptable tel que le résultat net, l'EBITDA ou le chiffre d'affaires, par rapport à des entreprises similaires du même secteur.

35 Voir, à titre d'exemple, les données sectorielles publiées par Aswath Damodaran, spécialiste reconnu de l'évaluation financière à la NYU Stern School of Business. https://pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/vebitda.html

étayée par des recherches empiriques publiées (Wang et Hou, 2025).
Pour les entreprises qui détiennent d'importants volumes de données, **elle contribue à expliquer et à justifier la création de valeur lors d'une opération, même lorsque la valeur des données n'est que partiellement reflétée dans les cours des actions et la valeur comptable.**

Les secteurs fortement dépendants des données sont davantage concentrés, bénéficient d'économies d'échelle plus importantes et maintiennent des niveaux de rentabilité plus élevés sur le long terme. Cela conduit à des multiples plus élevés que dans les secteurs traditionnels, moins exposés aux données. Les éléments disponibles indiquent que les multiples sont relativement élevés dans les secteurs des logiciels, de la publicité numérique, de l'intelligence artificielle (IA), des fintechs et de la santé, tandis qu'ils sont faibles dans les secteurs du commerce, de l'agroalimentaire, de l'énergie et de l'industrie manufacturière.

En outre, l'évaluation de la valeur économique des données aide également à reconsidérer les coûts de mise en conformité, qui sont souvent, à défaut, traités comme des charges d'exploitation. **Les dépenses de mise en conformité présentent les caractéristiques d'un investissement et peuvent donc être traitées comme telles.** Elles peuvent prendre la forme de dépenses de R&D ou de dépenses d'investissement (capex), sont mobilisées dans le cadre du cycle d'activité de l'entreprise et génèrent de la valeur future, comme indiqué dans la section 3.2.

Lors de notre atelier, il est apparu que **plus la due diligence est granulaire, en s'appuyant sur les ensembles de données détenus par une entreprise, leurs finalités, leur contenu et leur cycle de vie, plus le lien avec la rentabilité de l'activité est étroit et plus l'impact sur la création de valeur est important.** Il en va de même pour les risques liés aux données, qui devraient être identifiés de manière spécifique, par exemple à l'aide de l'analyse d'impact relative à la protection des données (AIPD).

Les risques liés aux données peuvent affecter la valeur de l'entreprise à différents niveaux. Ils peuvent avoir une incidence sur la rentabilité de l'activité à court terme, par exemple lorsqu'une entreprise est victime d'une violation de données ou lorsque sa réputation est affectée par un traitement de données non conforme ou par une procédure de sanction engagée par une autorité de protection des données. Ces incidents peuvent avoir des effets à court terme, susceptibles de s'estomper à plus long terme. Ils comportent également une dimension à long terme. Par exemple, les violations de données peuvent produire des effets indirects, tels qu'une prise de conscience accrue du public aux risques liés aux données, susceptible d'entraîner un renforcement de la réglementation, ou encore une perte de confiance du public à l'égard des entreprises technologiques et d'intelligence artificielle (IA). Ces types de risques liés aux données sont susceptibles de modifier à la fois les conditions de marché et la confiance du public.

En ce qui concerne l'accès au financement, il est établi que les secteurs fortement dépendants des données (et, plus généralement, les secteurs riches en actifs incorporels) font face à un **déficit de financement, en raison des difficultés d'évaluation des actifs incorporels et de l'absence d'indicateurs sur la conformité à la protection des données susceptibles d'éclairer les décisions de financement** (OCDE, 2021). Ces entreprises sont moins en mesure de donner leurs actifs en garantie et l'asymétrie d'information concernant l'évaluation financière de leurs actifs est plus forte (faute de transparence sur les bénéfices et les risques liés à leurs données). Par conséquent, elles ont d'avantage tendance à recourir à un financement sur fonds propres. Cela est particulièrement vrai dans le secteur technologique.

L'impact de l'intégration des opportunités et des risques liés aux données dans l'évaluation financière d'une entreprise, qui dépend également de son ancienneté et de sa position sur le marché, peut être résumée comme suit :

Impact sur la rentabilité de l'entreprise	Impact sur les conditions de financement
Les modèles économiques fondés sur la donnée génèrent des gains de rentabilité élevés et plus stables, reflétés dans des flux de trésorerie futurs plus importants (court terme). Une bonne gestion et une bonne gouvernance des données contribuent à sécuriser la performance et à réduire les risques (court terme). L'effet est amplifié lorsque l'entreprise est mature et bénéficie d'une position de marché établie. Les risques liés aux données, s'ils ne sont pas atténués, affectent la rentabilité future (court terme) ainsi que le potentiel de croissance de long terme de l'entreprise.	L'effet de l'exposition des données sur le coût des fonds propres est ambigu : une rentabilité plus élevée réduit le coût des fonds propres, toutes choses égales par ailleurs. Les risques liés aux données tendent à accroître la prime de risque incluse dans le coût des fonds propres, en particulier si l'entreprise est jeune (l'incertitude étant alors plus élevée). L'effet net dépend du stade de développement et de la position de marché de l'entreprise. Le manque de quantification cohérente de la valeur des actifs de données augmente le coût de l'endettement et rend plus difficile l'accès au financement des entreprises (asymétrie d'information).

Tableau 3 : l'impact des données sur la valeur économique et les conditions de financement d'une entreprise

Ce tableau permet également de comprendre pourquoi **une meilleure intégration des opportunités et des risques liés aux données dans les référentiels comptables, ainsi qu'une plus grande transparence de la part des émetteurs concernant leurs politiques en matière de données, comme le proposent le présent rapport, auraient un effet positif sur le financement de l'innovation.**

3.3.6 Intégration des questions de données dans la méthode des flux de trésorerie actualisés

Nous avons utilisé la méthode des flux de trésorerie actualisés (Discounted Cash Flow, DCF), afin de montrer qu'il est possible de mieux intégrer les aspects liés aux données dans les évaluations financières. Le modèle DCF, en tant que méthode d'évaluation financière basée sur les flux de trésorerie futurs générés par une entreprise, actualise ces flux

en fonction du coût du capital. **Il est pertinent dans la mesure où il intègre à la fois les effets sur la rentabilité et les effets pénalisants des risques.**

L'approche présentée ci-dessous est une vue d'ensemble. Son application devrait être précisée selon le type d'entreprise, la nature des risques et l'intégration des aspects fiscaux et d'investissement. Nous souhaiterions poursuivre les discussions avec les acteurs des fusions-acquisitions sur l'utilisation et l'application de cette approche.

La **valeur économique d'une entreprise** est calculée (par opposition à la valeur comptable de ses actifs) sur la base des revenus générés à un horizon temporel donné (généralement, l'horizon du plan d'affaires). Cette valeur économique se reflète dans la valeur des fonds propres et dans la valeur de la dette (par opposition à leurs valeurs comptables du côté passif) :

VE = VOF + VD

Où VE est la valeur économique d'une entreprise, VOF est la valeur de ses fonds propres et VD est la valeur de sa dette.

Le coût moyen pondéré du capital (WACC joue un rôle important dans le calcul. Il dépend également de la structure de financement et est défini comme suit :

$$\text{WACC} = \frac{V_{OF}}{V_{OF} + V_D} K_{OF} + \frac{V_D}{V_{OF} + V_D} K_D$$

où K_{OF} reflète une prime de risque spécifique à l'entreprise (voir tableau 2) et D un spread de crédit (toujours plus élevé pour les entreprises à forte intensité de données). L'effet de la fiscalité est ici négligé.

Les risques liés aux données sont donc davantage susceptibles d'avoir une incidence sur le WACC, lorsque l'entreprise est jeune et son marché est plus concurrentiel. Il est par conséquent raisonnable d'intégrer les risques de court terme liés aux données dans le choix d'un WACC plus élevé pour ces entreprises.

La valeur économique est la somme des flux de trésorerie futurs (FCFi), actualisés au moyen du WACC, **et d'une valeur finale** (FV) qui dépend d'hypothèses concernant la rentabilité à long terme et le taux de croissance à long terme de l'entreprise. Cette valeur finale constitue une composante importante de l'estimation de la valeur économique et est parfois difficile à justifier. **Il est donc raisonnable d'intégrer les risques liés aux données à long terme dans le calcul de la valeur finale** afin de refléter les effets de ces risques sur la rentabilité à long terme et le taux de croissance à long terme ; cette prise en compte réduit la valeur finale.

$$VE = \sum_{i=1}^{n} \frac{FCFi}{(1+WACC)^i} + \frac{FV}{(1+WACC)^n}$$

Sur la base d'un horizon donné du plan d'affaires et d'une structure de financement donnée, les effets positifs de la dépendance aux données sur la rentabilité sont pris en compte, avec **une majoration lorsque la gestion responsable des données et la gouvernance des données sont correctement assurées**. Par exemple, lorsqu'une certification en matière de protection de la vie privée est obtenue, celle-ci pourrait être intégrée dans les flux de trésorerie futurs (FCF).

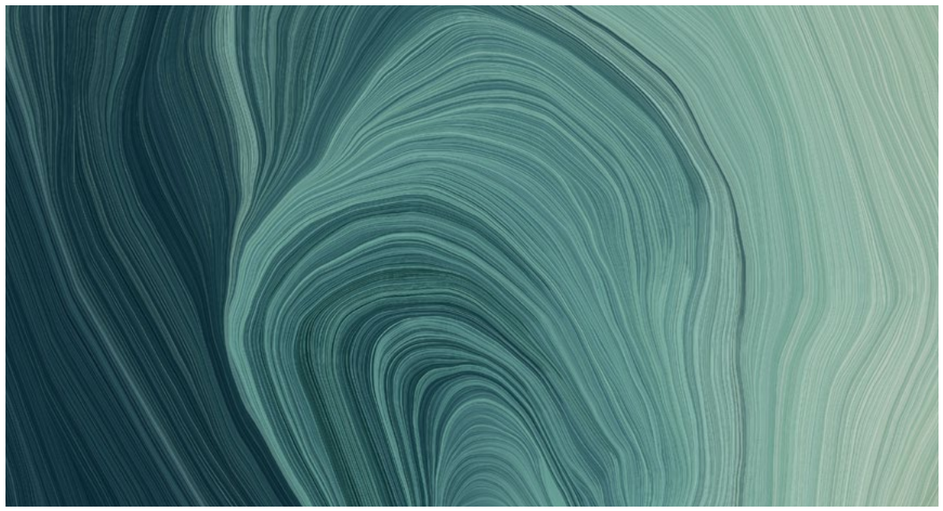
La détection d'une non-conformité ou de pratiques insuffisante en matière de gestion des données et de gouvernance des données dans l'entreprise réduirait cet avantage.

La valeur finale (FV) serait affectée par les risques liés aux données à long terme, tels que les risques sociétaux et cyber, qui sont généraux et non diversifiables. Cette approche contribue également à rendre la valeur finale plus réaliste.

Dans cette approche, le WACC ne serait pas systématiquement pénalisé. Mais il augmenterait avec les risques identifiés en matière de données, comme on l'a vu, en particulier pour les entreprises plus jeunes et celles qui opèrent sur des marchés plus concurrentiels. IL pourrait également être affectée par d'autres considérations relatives aux données propres à l'entreprise, telles que la nécessité de réaliser des investissements en matière de conformité ou de cybersécurité.

Des analyses de sensibilité peuvent compléter l'estimation de la valeur économique, afin de tester l'impact de la survenance d'un risque de données donné. Ces analyses permettraient d'évaluer l'impact spécifique du risque à court terme, sans pénaliser la valeur économique dans l'estimation centrale. La réalisation de tests de sensibilité, parallèlement à l'estimation de la valeur économique, peut également être utilisée comme un outil interne de gestion des risques, afin d'éclairer les décisions relatives aux investissements en matière de conformité. La valeur économique et les tests de sensibilité peuvent être communiqués aux assureurs et aux agences de notation et servir de support aux échanges avec eux. Dans les cas où le modèle économique est fortement dépendant des données, elles peuvent également être utilisées comme outil de stress test.

Les développements présentés dans cette section montrent que l'évaluation financière des actifs de données et des risques liés aux données est essentielle à la création de valeur dans l'économie numérique. Elle permet de réduire les asymétries d'information dans les transactions et d'accroître les possibilités de financement.



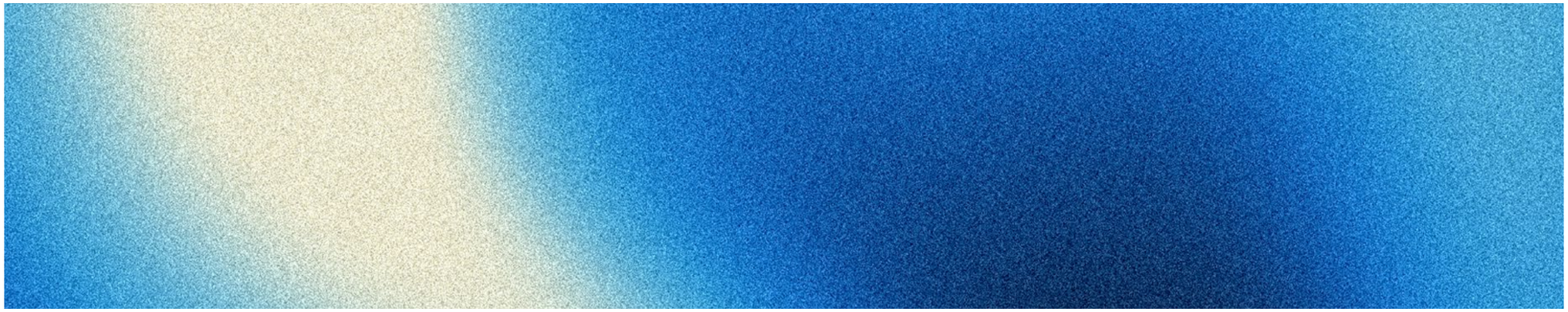
4. Bonnes pratiques émergentes

Ce rapport présente les résultats de l'étude, fondés sur les échanges avec des organisations du secteur financier dans le cadre d'entretiens semi-directifs et d'ateliers, sur l'analyse des référentiels ESG et comptables, ainsi que sur les résultats d'enquêtes quantitatives menées au Luxembourg et en France. Cette section synthétise les conclusions relatives à la valeur de la conformité en matière de protection des données dans le secteur financier et présente les bonnes pratiques émergentes autour de trois thèmes : la comptabilité, l'évaluation financière et la gouvernance, le risque cyber et l'IA.

Bonnes pratiques comptables

1. À mesure que les organisations s'appuient de plus en plus sur des bases de données générées en interne, y compris celles contenant des données personnelles, la **possibilité de comptabiliser ces bases de données en tant qu'actifs mérite d'être examinée au cas par cas.** Cette question est particulièrement pertinente lorsque les bases de données sont bien structurées et font l'objet d'une gouvernance appropriée, car les bases de données non conformes peuvent entraîner des risques juridiques, opérationnels et liés à leur évaluation, susceptibles de limiter leur utilisation et leur valeur économique. La cartographie des bases de données permet aux organisations de comprendre quelles données à caractère personnel elles détiennent et leur donne la possibilité d'évaluer et d'améliorer la qualité de ces jeux de données, en appliquant, lorsque cela est pertinent, des principes de protection des données tels que l'exactitude des données et la minimisation des données. L'examen des pratiques actuelles en matière de d'évaluation et des référentiels comptables permet également aux organisations de **réexaminer le statut de leurs jeux de données** au regard des critères de la norme IAS 38 et de leur évaluation en tant qu'immobilisations incorporelles.

2. Les organisations auraient **intérêt à intégrer les cadres de protection des données dans leurs pratiques comptables.** L'intégration des exigences en matière de conformité à la réglementation sur la protection des données (base juridique, durées de conservation, exactitude des données, etc.) dans les pratiques comptables peut constituer un cadre de référence. L'application des principes de protection des données aux pratiques comptables et l'implication des délégués à la



protection des données (DPO) dans le processus comptable facilitent l'amélioration de la communication et permettent de créer une compréhension commune de la manière de comptabiliser et d'évaluer les jeux de données en tant qu'actifs stratégiques. Une telle approche peut contribuer à **une prise de décision plus solide** en garantissant que les jeux de données pris en compte dans les évaluations, les transactions ou les initiatives stratégiques respectent les exigences juridiques, de qualité et de gouvernance nécessaires à la création et au maintien de la valeur pour l'entreprise.

3. Les parties prenantes aux opérations de fusions-acquisitions, les auditeurs et les agences de notation prennent de plus en plus en compte **les risques liés aux données** lorsqu'ils évaluent la valeur des actifs constitués de données personnelles. L'évaluation des actifs liés aux données personnelles devrait être réexaminée régulièrement et, le cas échéant, étayée par des **tests de dépréciation**. Ces réexamens peuvent aider les organisations à disposer d'une compréhension à jour de leurs jeux de données, à identifier les risques juridiques, opérationnels ou liés à la cybersécurité susceptibles d'affecter leur valeur, et à garantir que les jeux de données utilisés dans les activités de l'entreprise et les applications d'IA restent fiables, conformes et adaptés à leur finalité.

4. Les résultats de l'étude et l'analyse des normes comptables internationales ont montré que la **mise à jour de la norme IAS 38** faciliterait l'évaluation des jeux de données contenant des données personnelles en tant qu'immobilisations incorporelles. La norme IAS 38 date de 2001 et a été mise à jour à plusieurs reprises afin de tenir compte de l'évolution du contexte. Une nouvelle révision permettrait donc de garantir qu'elle prenne en compte l'économie fondée sur les données, dans laquelle les données constituent un actif incorporel. Un dialogue entre les autorités de régulation et les organismes chargés de normalisation contribuerait à évaluer la faisabilité d'une telle évolution et à définir une approche proportionnée et appropriée.

Bonnes pratiques en matière d'évaluation financière

5. Les organisations commencent à adopter une approche plus intégrée de l'évaluation de la valeur des données, **en prenant en compte à la fois les avantages et les coûts** associés à la collecte, à l'utilisation et au stockage des données ainsi qu'au respect des exigences en matière de protection des données, parallèlement aux risques découlant d'une faible qualité des données, du non-respect des exigences ou d'incidents de cybersécurité. **L'intégration des considérations liées aux données dans les processus d'évaluation** peut offrir une vision plus complète des facteurs qui influent sur la valeur économique des jeux de données. Une telle approche peut contribuer à une prise de décision mieux éclairée, aider les organisations à identifier et à atténuer les risques liés aux données et à la cybersécurité, et offrir une vision plus équilibrée des effets du respect des exigences en matière de protection des données dans les évaluations stratégiques et financières. Bien que tous ces effets ne se reflètent pas nécessairement directement dans les bilans, ils peuvent contribuer à la création de valeur à plus long terme. La capacité à évaluer des risques, tels que la qualité des données, et des avantages, tels que la confiance, qui sont difficiles à quantifier, peut fournir aux organisations des indicateurs utiles dans leurs échanges avec les investisseurs, les consommateurs et les autorités de régulation.

6. Les organisations intègrent et documentent leur évaluation de la conformité en matière de protection des données à caractère personnel **dans le cadre de leurs procédures de due diligence** relatives aux transactions financières. Dans le cadre des opérations de fusion-acquisition et des opérations d'investissement, cette documentation contribue à identifier et à évaluer les enjeux liés à la conformité en matière de protection des données, renforçant ainsi la transparence et la confiance dans le processus de prise de décision. Cela permet aux acquéreurs, aux investisseurs et aux autres parties prenantes impliquées dans les transactions financières d'accéder, tout au long du processus de due diligence, aux informations pertinentes relatives à la conformité en matière de protection des données et aux risques liés aux données.

7. Les méthodes d'évaluation et les référentiels comptables reposent souvent sur des **estimations des flux de trésorerie futurs**, complétées par des analyses de sensibilité. La conformité en matière de protection des données et les risques liés aux données peuvent être intégrés aux évaluations selon la méthode des flux de trésorerie actualisés (**Discounted Cash Flow - DCF),** en évaluant leur incidence potentielle sur les flux de trésorerie futurs et la création de valeur. De même, les méthodes d'évaluation fondées sur les cash flows et sur l'exonération des redevances tiennent compte des avantages futurs attendus. Dans ce contexte, la norme IAS 36 définit la valeur d'utilité comme la valeur actuelle des flux de trésorerie futurs estimés.

8. Les acteurs du marché qui participent à des opérations de fusion-acquisition ou les accompagnent reconnaissent que la démonstration de la conformité en matière de protection des données dans le cadre d'une transaction financière peut nécessiter une **feuille de route structurée permettant de remédier aux lacunes en matière de conformité et aux risques liés aux données identifiés**. Dans le cadre des opérations de fusion-acquisition, les entreprises peuvent avoir besoin de temps pour remédier à ces lacunes (par exemple en mettant à niveau leurs systèmes informatiques et en renforçant leurs pratiques de gestion des données personnelles). Une telle feuille de route peut créer les conditions nécessaires à la création de valeur, y compris après la transaction, tout en contribuant à réduire le coût des garanties de passif.

Bonnes pratiques en matière de gouvernance, de cybersécurité et d'IA

9. Les organisations adoptent de plus en plus **une approche stratégique de la conformité en matière de protection des données, en la considérant comme un actif** de l'entreprise. Les organisations qui détiennent d'importants volumes de données personnelles et disposent d'une stratégie claire en matière de données, y compris pour les données personnelles, sont les mieux à même d'atténuer les risques stratégiques, opérationnels et liés à la cybersécurité et de tirer parti des bénéfices liés à la conformité. Il est essentiel, pour développer une approche stratégique, de veiller à ce que les décideurs de haut niveau et le conseil d'administration disposent d'une stratégie écrite en matière de données et de conformité, et de **mettre en place des indicateurs clés de performance (KPI)** reflétant la valeur des données personnelles et de la conformité.

10. Les organisations commencent à reconnaître l'importance d'intégrer la protection des données dans les dispositifs de gouvernance organisationnelle et de la gouvernance de l'IA. Lorsque les données générées en interne sont essentielles au développement et au déploiement de l'IA, l'intégration de la protection des données dans les cadres de gouvernance organisationnelle et de gouvernance de l'IA améliore l'efficacité, réduit les risques et garantit la cohérence des pratiques. Les organisations ont constaté qu'il pouvait être bénéfique de **développer, au sein des équipes de DPO, des fonctions dédiées à l'IA et à l'éthique** afin de soutenir un déploiement et une gouvernance plus larges de l'IA.

11. Les organisations **intègrent les règles de protection des données dans leurs stratégies de cyberrésilience**. Il s'agit de la pratique la plus établie en matière de prise en compte des données dans les stratégies organisationnelles. Dans le cadre de ces stratégies, les organisations modélisent les conséquences financières et réputationnelles des violations de données et des incidents cyber afin d'améliorer leur préparation, d'orienter les investissements en cybersécurité et de réduire les répercussions potentielles sur les performances de l'entreprise et sa perception par le marché. Cela comprend la quantification des risques liés à la protection des données et la réalisation de tests de résistance cyber simulant des violations de données et des incidents majeurs en matière de protection de la vie privée afin d'en évaluer les impacts. L'intégration d'indicateurs relatifs à la protection des données dans le reporting sur les risques cyber fournit également au conseil d'administration une vision globale des risques liés à la cybersécurité et à la protection des données.

12. Les organisations peuvent **tirer parti des avantages liés aux certifications en matière de protection des données**. Les indicateurs de conformité, tels que les certifications en matière de protection des données et les codes de conduite approuvés, contribuent à démontrer la conformité et à la transformer en avantage concurrentiel. Dans le contexte de la détention, de l'évaluation et de la comptabilisation des actifs de données, les certifications en matière de protection des données peuvent apporter une assurance que les activités de traitement sont conformes aux exigences applicables en matière de protection des données. Cela renforce la confiance dans la licéité, l'intégrité et la possibilité d'utiliser durablement les actifs de données, y compris ceux qui sous-tendent les systèmes d'IA et les services utilisant l'IA. Dans le contexte des fusions-acquisitions et opérations d'investissement, les certifications en matière de protection des données facilitent également les procédures de due diligence en apportant des éléments de preuve indépendants de la conformité et en aidant les parties prenantes à évaluer les risques liés à la protection de la vie privée, les responsabilités et la pérennité des actifs fondés sur les données et liés à l'IA.

5. Conclusion

Ce rapport a examiné les multiples usages et la valeur que la conformité en matière de protection des données apporte aux organisations actives sur les marchés financiers.

Bien que le respect des exigences en matière de protection des données, depuis la cartographie des données et les analyses d'impact relatives à la protection des données jusqu'à la mise en œuvre de mesures de protection techniques et organisationnelles, puisse représenter un effort opérationnel et financier important, en particulier pour les petites organisations, l'analyse présentée dans ce rapport suggère que **ces coûts devraient être considérés comme un investissement.** En effet, ils doivent être mis en regard des avantages tangibles qu'offrent de solides pratiques de protection des données, notamment un renforcement de la confiance des clients, une réduction de l'exposition aux risques réputationnels et juridiques, une plus grande résilience opérationnelle, une augmentation de la valeur des jeux de données et une base plus solide pour une innovation numérique durable.

L'un des principaux enseignements de ce rapport est la reconnaissance croissante des données en tant qu'actif stratégique. Les organisations financières s'appuient de plus en plus sur la collecte, le traitement et l'analyse des données à caractère personnel pour développer de nouveaux produits, affiner les modèles de risque et personnaliser leurs services. **Cette évolution nécessite une transformation parallèle de la manière dont les organisations appréhendent la conformité,** qui ne doit plus être perçue uniquement comme une obligation réglementaire défensive, mais également comme une opportunité de mettre en place des structures de gouvernance permettant de libérer la valeur des données de manière responsable. Les organisations qui intègrent des principes de protection des données, tels que la minimisation des données, la limitation des finalités et la protection des données dès la conception, dans leur stratégie globale en matière de données sont mieux placées pour tirer parti de cette valeur, tout en préservant la confiance de leurs investisseurs, de leurs clients et des autorités de régulation.

Ce rapport est le fruit d'une coopération renforcée entre la CNPD, la CNIL et l'ICO, et a contribué à développer **une compréhension commune de la conformité** en matière de protection des données au sein des organisations financières de ces

trois marchés. Le renforcement de ces canaux de coopération demeure essentiel pour approfondir les connaissances relatives à l'application des règles de protection des données dans les différents marchés.

Dans le même ordre d'idées, il est de plus en plus reconnu que la protection des données constitue une pierre angulaire de la confiance et de la stabilité des organisations financières et, plus largement, de l'écosystème financier. À mesure que les services financiers deviennent de plus en plus dépendants des données et interconnectés, englobant les banques, les assureurs, les prestataires de services fintech et les prestataires de services tiers, la protection des données personnelles sous-tend la sécurité et l'intégrité de l'ensemble du système. **Des faiblesses dans la gouvernance des données ou dans les pratiques de protection des données,** à quelque niveau que ce soit de cet écosystème, **peuvent avoir des effets en cascade**, érodant la confiance des consommateurs et exposant les organisations à un risque systémique. Garantir des pratiques solides et cohérentes en matière de protection des données ne relève donc pas uniquement de la conformité propre à chaque organisation, mais constitue une responsabilité partagée qui contribue à la résilience de l'ensemble du secteur financier.

Enfin, ce rapport s'appuie sur les éléments recueillis au moyen d'enquêtes et **d'un dialogue ouvert avec les parties prenantes**. Ces échanges apportent un éclairage précieux sur les difficultés concrètes auxquelles les organismes sont confrontés pour se mettre en conformité, tout en faisant émerger des risques et des bonnes pratiques qui pourraient autrement passer inaperçus. Les enseignements tirés de ces échanges permettent tant aux aux autorités de régulation qu'aux organisations d'affiner progressivement leurs approches, afin de garantir que les cadres réglementaires restent proportionnés, applicables et adaptés à l'évolution rapide de l'environnement des données, tout en permettant aux organisations d'innover et de se développer.

***

6. Références

Aboody, D. & Lev, B., 1998. The value relevance of intangibles: The case of software capitalization.. Journal of Accounting Research, Volume 36, pp. 161-191.

Babina, T., Anastassia, F., He, A. & Hodson, J., 2024. Artificial intelligence, firm growth, and product innovation. Journal of Financial Economics, Volume 151.

Blycha, N. A. et al., 2026. Pricing the Unpriced Asset: A Standards-Based Method for Valuing Enterprise Data under IAS 38 and IAS 2,

Ceddaha, F., 2025. Fusions-Acquisitions. 7ème éd. Paris: Economica, 2025, 506 p.

Cheong, H., Kim, B. & Vaquero, I. U., 2023. A Data Valuation Model to Estimate the Investment Value of Platform Companies: Based on Discounted Cash Flow. Journal of Risk and Finanical Management , 16(6).

Conseil national de la productivité, 2023. Rapport Annual 2022-2023. [En ligne]
Available at: https://odc.gouvernement.lu/dam-assets/domaines/cnp/cnp-rapport-2022-2023.pdf

Day, K. & Booker, Q., 2024. Market Reactions to Cybersecurity Incidents: A Case Study Approach. Issues in Information Systems, pp. 260-276.

Deloitte, 2025. Valuing data assets can be key to unlocking board-level support for data modernization and transformation,

Department for Business and Trade, 2024. UK Sustainability Reporting Standards. [En ligne]
Disponible à l'adresse : https://www.gov.uk/guidance/uk-sustainability-reporting-standards

Ding, R., 2016. Disclosure of Downside Risk and Investors' Use of Qualitative Information: Evidence from the IPO Prospectus's Risk Factor Section. International Review of Finance, 16(1).

EFRAG, 2021. Better Information on Intangibles – Which is the Best Way to Go?

EU 2022/2557, 2022. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance).

EU Commission, 2022. Directive (EU)

2022/2464. [En ligne]
Disponible à l'adresse : https://eur-lex.europa.eu/eli/dir/2022/2464/oj/eng

Farboodi, M., Singal, D., Veldkamp, L. & Venkateswaren, V., 2025. Valuing Financial Data. The Review of Financial Studies, 38(3), pp. 938-980.

Frontier Economics, 2021. The value of data assets: A report fro the department of culture, media and sport Disponible à l'adresse : https://assets.publishing.service.gov.uk/media/6399f93d8fa8f50de138f220/Frontier_Economics_-_value_of_data_assets_-_Dec_2021.pdf

Gao, X., Liu, J. & Lu, H., 2025. Accounting for Data Assets (Working Paper)

Guo, X., Li, P. & Wang, F., 2026. How do data assets enhance firm value in the digital economy: Evidence from listed tech firms. Financial Research Letters.

IAASB, 2016. ISA 250 (Revised), Consideration of Laws and Regulations in an Audit of Financial Statements.
Disponible à l'adresse : https://www.iaasb.org/publications/isa-250-revised-consideration-laws-and-regulations-audit-financial-statements-13

ICAEW, 2025. A new emergening type of intangible.
Disponible à l'adresse : https://www.icaew.com/-/media/corporate/files/policy-and-research/research-and-academics/data---a-new-emerging-type-of-intangibles.ashx

ICO, 2026. Data Controller Study.
Disponible à l'adresse : https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/data-controller-study/

Iron Mountain & De Braw Blackstone Westbroek, 2013. European Document Retention Guide

Kepler, J., McClure, C. & Stewart, C., 2026. Competition Enforcement and Accounting for Intangible Capital. The Journal of Finance.

Lev, B., 2018. The deteriorating usefulness of financial report information and how to reverse it.. Accounting and Business Research, 48(5), pp. 465-493.

Lev, B. & Gu, F., 2016. The End of Accounting and the Path Forward for Investors and Managers:Wiley.

Lev, B. & Sougiannis, T., 1996. The capitalization, amortization, and value-relevance of R&D. Journal of Accouting and Economics, 21(1), pp. 107-138.

Lev, B. & Zarowin, P., 1999. The Boundaries of Financial Reporting and How to Extend Them. Journal of Accounting Research, 37(2), pp. 353-385.

Li, K. & McClure, C., 2023. Evolution in Value Relevance of Accounting Information. The Accounting Review, 98(1), pp. 1-28.

Martins, A. M., Moutinho, N. & Cro, S., 2025. Stock market effects of major cyber-attacks: evidence for breached and cybersecurity listed firms. Journal of Banking Regulation, 26(868–877).

Muktadir-Al-Mukit, D. & Ali, H., 2025. The Dynamics of Stock Market Responses Following the Cyber-Attacks News: Evidence from Event Study. Information Systems Frontiers.

National Protective Security Authority, 2026. About us: Critical National Infrastructure.

OECD, 2021. Mind the financing gap : Enhancing the contribution of intangible assets to productivity : Economics Department Working Paper

OECD, 2022. Measuring the value of Data and Data flows: OECD Digital Economy Papers 345.

OECD, 2022. Measuring data as an asset : Framework, methods and preliminary estimates : OECD Economics Department Working Paper No 1731.

PWC, 2026. Global Top 100 companies by market capitalisation : March 2026,

Sargent, T. & Denniston, L., 2023. Valuing Data: Where Are We, and Where Do We Go Next?. Center for International Governance Innovation, Volume 280.

Schoch, D. S., 2020. Mergers and Acquisitions in the Data Economy. [En ligne]
Disponible à l'adresse : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3686247

Skinner, D., 2008. Accounting for intangibles – a critical review of policy recommendations. Accounting and Business Research, Volume 38, pp. 191-204.

Tambe, P., Hitt, L., Rock, D. & Brynjolfsson, E., 2020. Digital Capital and Superstar Firms. National Bureau of Economic Research Working Papers, Volume 28285.

Veldkamp, L., 2023. Valuing Data as an Asset. Review of Finance, 27(5), p. 1545–1562.

Wang, S. & Hou, L., 2025. Data assetization and corporate capital pricing efficiency. Financial Research Letters, Volume 86.

World Economic Forum, 2026. The Future of Venture Capital: Unlocking Liquidity and Growth, Insight Report.
Disponible à l'adresse : https://reports.weforum.org/docs/WEF_The_Future_of_Venture_Capital_2026.pdf

Wyatt, A., 2008. What financial and non-financial information on intangibles is value-relevant? A review of the evidence. Accounting and Business Research, Volume 38, pp. 217-256.

Xiaochuan, G., Pencheng, L. & Wang, F., 2026. How do data assets enhance firm value in the digital economy: Evidence from listed tech firms. Financial Research Letters, Volume 91.

Xiao, S., Wu, K., Xiao, X. & Changqui, L., 2025. How do data assets affect firm investment?. International review of financial analysis, Volume 106, pp. 1-12.

Annexes :

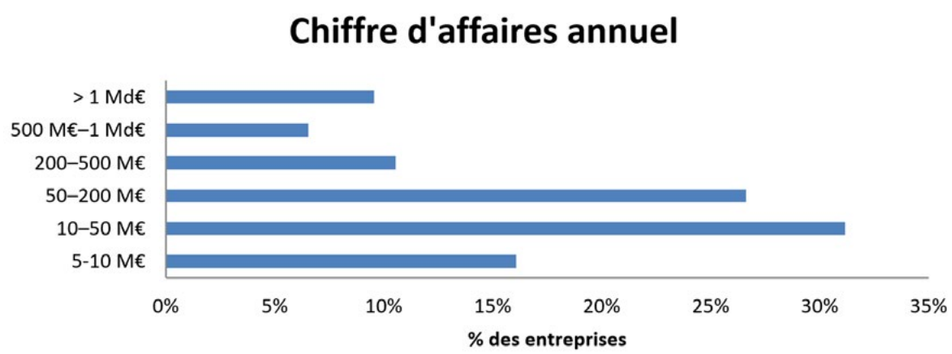
A. Résultats statistiques

1. Méthodologie

L'enquête a recueilli 204 réponses émanant d'entreprises variées. Elle a été diffusée via Framaforms auprès d'organismes dotés d'un délégué à la protection des données (DPO), à partir des désignations de DPO enregistrées par la CNIL, croisées avec un registre public des entreprises.

Plusieurs éléments relatifs aux données doivent être gardés à l'esprit lors de la lecture des résultats. Premièrement, la plupart des questions étaient à choix multiples : une même entreprise pouvait sélectionner plusieurs réponses et donc présenter simultanément plusieurs caractéristiques. Afin de faciliter la lecture des résultats, les pourcentages sont par conséquent calculés uniquement sur la base du nombre d'entreprises ayant répondu à la question concernée, et non sur la base du nombre total de réponses à cette question. Chaque pourcentage peut ainsi se lire comme « X % des entreprises ayant répondu à cette question… ». En conséquence, les pourcentages d'une même question peuvent totaliser plus de 100 %. Deuxièmement, toutes les entreprises n'ont pas rempli l'intégralité du questionnaire : le nombre de répondants varie donc légèrement d'une question à l'autre, et chaque résultat est calculé uniquement sur les entreprises ayant effectivement répondu à la question concernée. Enfin, tous les liens statistiques présentés, ci-après, sont mesurés au moyen de tests appropriés et doivent être compris comme des corrélations et non comme des relations de causalité.

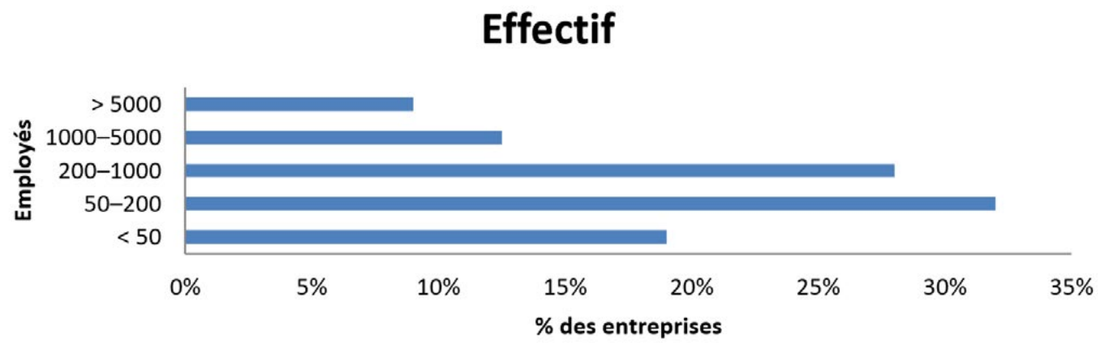
2. Profil des entreprises et modèles d'affaires



Graphique 4 Chiffre d'affaires annuel moyen

Le profil des répondants dessine un échantillon dominé par les **PME et les ETI**. Près de la moitié réalisent un chiffre d'affaires inférieur à 50 M€ (16 % en dessous de 10 M€ et 31 % entre 10 et 50 M€), tandis qu'un quart se situe dans la tranche 50-200 M€ ; les grandes entreprises restent minoritaires, seules 16 % dépassant 500 M€ de chiffre d'affaires et moins de 10 % dépassant le milliard d'euros.

La comparaison entre les entreprises contactées et les répondants révèle un biais de sélection lié à la taille, qu'il importe de rappeler lors de l'analyse des résultats : les entreprises réalisant plus de 200 millions d'euros de chiffre d'affaires, qui ne représentent que 10 % de l'échantillon, constituent 27 % des répondants ; la part de celles réalisant moins de 50 millions d'euros passe de 72 % à 47 %, et celle des entreprises réalisant moins de 10 millions d'euros de 35 % à 16 % (différence hautement significative). Les grandes entreprises, mieux dotées en fonctions DPO et financières, étaient donc plus susceptibles de répondre. L'échantillon surreprésente ainsi les grandes organisations, ce qui suggère que les résultats reflètent principalement les pratiques des moyennes et grandes entreprises.



Graphique 5 Nombre d'employés

La structure des effectifs confirme ce constat : un tiers des répondants emploient entre 50 et 200 salariés, et un peu plus d'un quart entre 200 et 1 000, tandis que les structures de plus de 5 000 personnes ne représentent que 9 % de l'échantillon.

Sur le plan géographique, l'Île-de-France concentre à elle seule plus d'un tiers des sièges sociaux (34,5 %), devant l'Auvergne-Rhône-Alpes (12,7 %), les autres régions se partageant le reste de manière plus diffuse.

Sur le plan sectoriel, l'échantillon est composé d'entreprises proposant des services divers (25 %), d'entreprises du secteur manufacturier (16 %), d'entreprises des secteurs financier ou des assurances (11 %), d'entreprises du commerce (10 %) suivies par celles des secteurs du transport, de la santé et de l'information-communication.

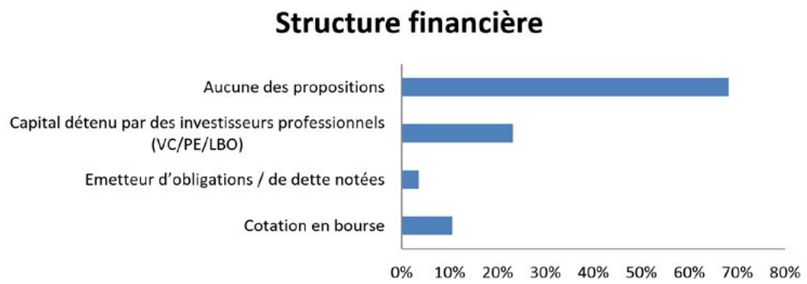
Les entreprises ont été invitées à préciser à quel niveau de leur organisation elles répondaient au questionnaire : DPO du groupe (40,7 %), « non concerné » (32,0 %), au

niveau de l'entreprise (30,9 %) et au niveau de la direction financière du groupe (20,6 %).

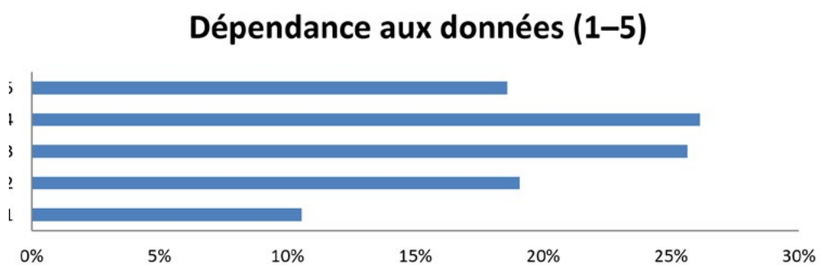
Un tiers des répondants se sont déclarés « non concernés » : il s'agit, selon toute vraisemblance, d'entreprises indépendantes n'appartenant pas à un groupe. Pour elles, la question du périmètre de la réponse est sans objet. En revanche, les deux autres niveaux relèvent d'un groupe et précisent la perspective de la réponse : le plus souvent celle du DPO du groupe (qui répond pour l'ensemble du groupe), parfois celle de l'entité seule. La combinaison de réponses la plus fréquente est DPO du groupe et direction financière du groupe (31 répondants), ce qui correspond à des groupes mieux structurés dans lesquels le répondant exerce à la fois le rôle de DPO du groupe et intervient dans le cadre d'un dispositif de consolidation au niveau du groupe.

Du point de vue financier, la majorité des répondants n'ont pas d'exposition directe aux marchés : plus des deux tiers (68 %) ne sont ni cotés, ni émetteurs de titres de créance, ni détenus par des investisseurs professionnels, tandis que 23 % ont un capital détenu par des fonds (capital-risque / capital-investissement / LBO) et 11 % sont cotés en bourse. Ces entreprises sont également familières des opérations de croissance externe, **puisque 37 % ont déjà réalisé une fusion-acquisition au cours des cinq dernières années.**

À noter que 43 % des entreprises appartenant à un groupe ont une exposition financière (cotation, dette, fonds), contre 11 % des entreprises indépendantes, et que 53 % des entreprises appartenant à un groupe ont participé à une opération de fusion-acquisition, contre 19 % des entreprises indépendantes.



Graphique 6 Structure financière



Graphique 7 Dépendance du modèle économique aux données

Interrogées sur la dépendance de leur modèle économique à l'égard des données, elles se situent en moyenne **à 3,23 sur une échelle de 1 à 5**, avec une répartition équilibrée : environ 30 % se déclarent peu dépendantes (niveaux 1-2), contre 45 % fortement dépendantes (niveaux 4 et 5).

Les réponses permettent de mieux comprendre la nature des données traitées ainsi que la manière dont la conformité est perçue au sein des entreprises. Près de trois entreprises sur quatre (71,5 %) déclarent traiter des données B2C courantes. Les données plus sensibles sont toutefois loin d'être marginales, puisque 37,5 % des répondants indiquent en traiter, tandis que les données comportementales et de profilage restent minoritaires (16,5 %). La part importante de réponses « autres » (26,5 %) s'explique notamment par les réponses textuelles des entreprises faisant état du traitement de données B2B.

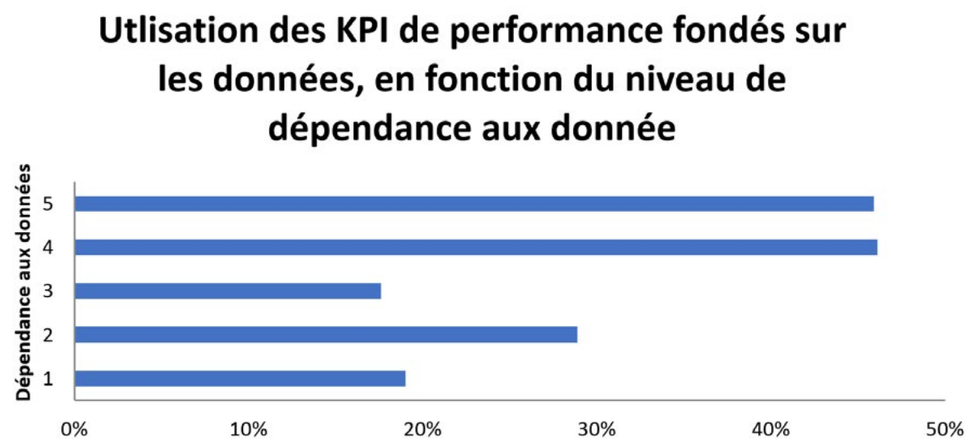
La perception de la conformité en matière de données est multiple : principalement considérée comme une question réglementaire et juridique, elle est également perçue par 57,5 % des répondants comme un facteur opérationnel ayant une incidence sur la réputation. La conformité « comme un atout » ou comme un avantage concurrentiel est reconnue par un peu plus d'un tiers des entreprises (34,5 %), **ce qui signifie qu'elles considèrent la protection des données comme un facteur créateur de valeur.**

3. Données et matérialité financière

3.1. Pilotage des données par des indicateurs

À la question : « Avez-vous mis en place des indicateurs clés de performance (KPI) spécifiques reliant la gouvernance des données et la performance financière ? »

65 % des répondants indiquent qu'ils ne disposent d'aucun KPI



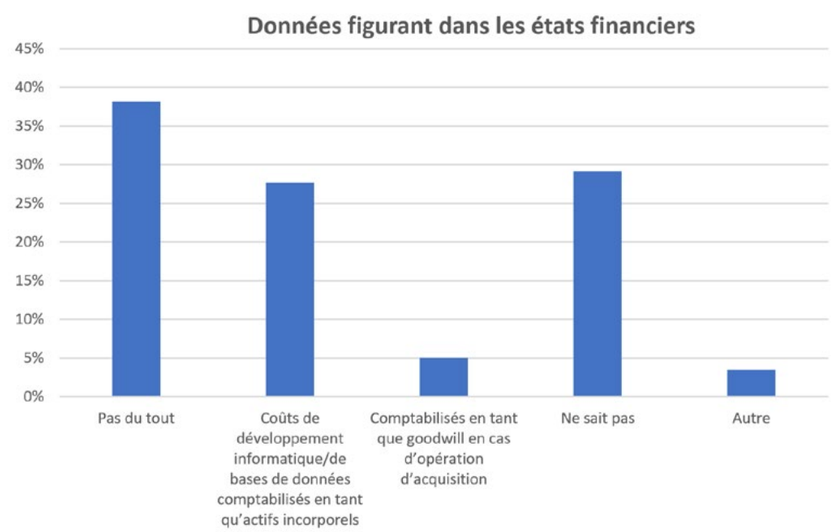
Graphique 8 Utilisation d'indicateurs clés de performance (KPI) fondés sur la dépendance aux données

établissant un lien entre les données et la performance. Lorsque des KPI existent, les répondants précisent que ces indicateurs sont principalement orientés vers les risques (24 %) et vers les clients et les ventes (11 %). Le recours à des KPI financiers liés aux données (6 % des réponses) reste rare.

Le lien qui se dessine entre la dépendance aux données et l'utilisation de KPI (au moins un parmi les indicateurs proposés) montre que les entreprises qui considèrent leur modèle économique comme fortement dépendant des données (niveaux 4 et 5) sont davantage susceptibles d'avoir mis en place des KPI liés à la performance des données (près de 46 %), contre 17 % à 29 % pour les entreprises moins dépendantes.

Plusieurs tests ont été réalisés pour valider ce résultat (corrélation de Spearman de 0,21, p = 0,003 ; test de tendance de Cochran-Armitage, p = 0,004). Une régression logistique indique que chaque point supplémentaire sur l'échelle de dépendance multiplie d'environ 1,45 les chances (odds ratio) de disposer de KPI. L'association est statistiquement robuste mais d'intensité modérée.

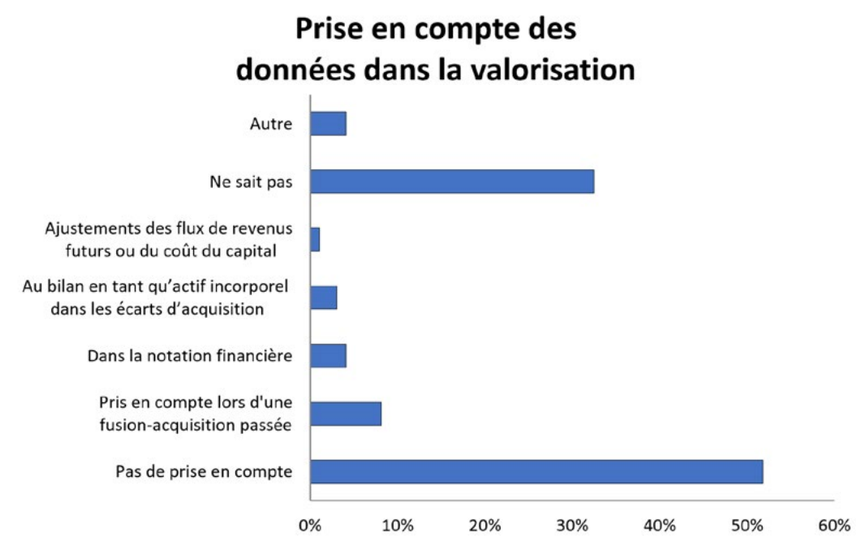
3.2 Intégration financière et comptable des données



Graphique 9 Modalités de prise en compte des données dans les états financiers

S'agissant de la prise en compte des données dans les états financiers, 38 % des entreprises considèrent que leurs bases de données n'y sont « pas du tout » reflétées, tandis que 29 % déclarent ne pas savoir, soit un total de 67 %. **Selon 28 % des répondants, les données sont intégrées aux états financiers sous la forme des coûts liés au développement informatique** et à la création des bases de données. L'intégration des données dans le goodwill (écart d'acquisition) lors d'une acquisition est mentionnée par 5 % des répondants.

S'agissant du Lien avec les opérations de fusion-acquisition, parmi les 199 entreprises ayant répondu à la question, celles qui avaient participé à une opération de fusion ou d'acquisition (82) étaient davantage susceptibles d'avoir intégré leurs bases de données dans leurs états financiers que celles n'ayant pas participé à une telle opération (117). Seules 26 % des entreprises ayant réalisé une opération de fusion ou d'acquisition ont indiqué que leurs données n'ont « pas du tout » prises en compte, contre 47 % des entreprises n'ayant pas participé à une acquisition (odds ratio = 0,39 et p = 0,003). Cette prise en compte se traduit principalement par l'immobilisation des coûts de développement (35 % contre 22 %, p = 0,05) et, dans une moindre mesure, par le goodwill (9 % contre 3 %, soit 7 sur 82 contre 3 sur 117). La différence observée concernant le goodwill n'est pas significative compte tenu du faible nombre de cas. Ces écarts reflètent en partie la taille plus importante des entreprises ayant participé à des opérations de fusion-acquisition. Après prise en compte de la taille des entreprises, la différence globale n'est plus statistiquement significative (OR ajusté = 1,8 ; p = 0,07).



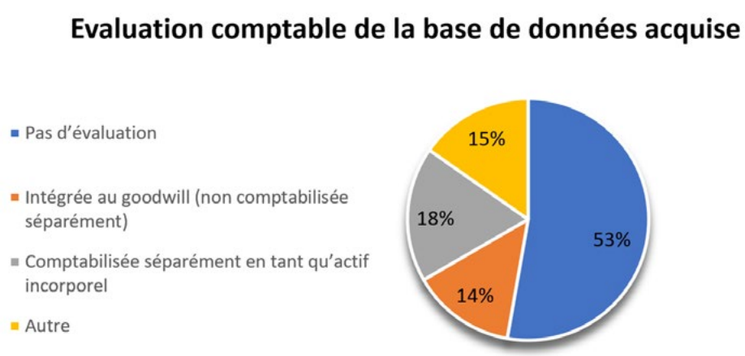
Graphique 10 Modalités de prise en compte des risques liés aux données dans les évaluations financières

Le graphique 10 présente les résultats de la question : « À votre connaissance, comment les risques liés aux données sont-ils principalement pris en compte dans l'évaluation financière de votre entreprise, que ce soit en interne ou par des acteurs externes ? » Plus de la moitié des répondants (52 %) indiquent qu'ils ne prennent pas du tout en compte les risques liés aux données, tandis que près d'un tiers (32 %) déclarent ne pas savoir. Les répondants indiquent que les risques liés aux données ont été pris en compte lors d'une opération de fusion-acquisition passée (8 %),

dans les notations financières (4 %), au bilan en tant qu'actif incorporel ou goodwill (3 %), ou encore par le biais d'un ajustement des flux de trésorerie futurs et du coût du capital (1 %).

Parmi les 197 entreprises ayant répondu, **celles ayant participé à une opération de fusion ou d'acquisition (82) étaient davantage susceptibles de prendre en compte les risques liés aux données dans leurs évaluations financières :** 22 %, contre 10 % pour les entreprises n'ayant pas participé à ce type d'opération (11 sur 115 ; odds ratio = 2,65 ; p = 0,024). Cet effet persiste après prise en compte de la taille des entreprises (OR ajusté = 2,6 ; intervalle de confiance de 1,1 à 6,5 ; p = 0,035).

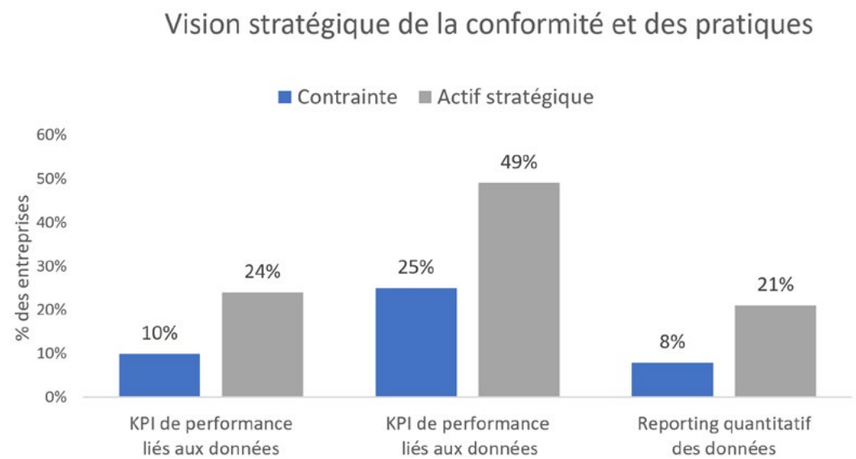
Cette question concerne uniquement les entreprises ayant participé à des opérations de fusion-acquisition. Au total, 72 répondants y ont répondu, soit un nombre inférieur aux 82 entreprises ayant déclaré avoir participé à une opération de fusion-acquisition à la question 15. Cette différence est cohérente avec la formulation de la question, qui porte sur l'intégration comptable des bases de données acquises et concerne donc principalement les acquéreurs plutôt que les cédants (voir annexe). Parmi ces 72 entreprises, plus de la moitié (38, soit 53 %) indiquent qu'aucune valorisation n'est réalisée. Lorsqu'une valorisation est effectuée, les répondants indiquent deux méthodes : **14 % (10 entreprises) intègrent les bases de données au goodwill, tandis que 18 % (13 entreprises) les identifient comme des actifs incorporels spécifiques dans leur bilan.** Ces résultats confortent les conclusions des questions 15 et 16 selon lesquelles le goodwill n'est pas le seul moyen de comptabiliser la valeur des données, y compris dans le contexte d'une acquisition. Les 15 % restants (11 réponses) relèvent de la catégorie « autre », qui traduit souvent une incertitude quant au sujet.



Graphique 11 Répondants ayant participé à des opérations de fusion-acquisition au cours des cinq dernières années, évaluation des bases de données acquises

Nous avons également demandé aux entreprises ayant participé à des opérations de fusion-acquisition si la découverte d'une base de données non conforme aurait pu avoir des conséquences financières directes. Dans près de la moitié des cas, les répondants indiquent que la découverte de bases de données non conformes n'a eu aucun impact. Dans 19 % des cas, elle a conduit à la mise en place de garanties spécifiques de responsabilité lors de la transaction, dans 4,5 % des cas à une révision à la baisse du prix de la transaction et, dans 3 % des cas, à l'annulation de la transaction. Plusieurs réponses en texte libre font apparaître un impact financier réel, bien qu'indirect : des coûts de mise en conformité répartis dans le temps, une baisse potentielle de la rentabilité ainsi que des risques identifiés après l'acquisition (violation de données au niveau de la force de vente, absence d'accord de DPA avec des sous-traitants) ont généré des coûts de remédiation et mobilisé les ressources des DPO.

3.3. Lien entre la vision des données et les pratiques financières



Graphique 12 Gouvernance des données et performance financière : perception et niveau d'intégration

Nous avons cherché à comprendre comment les entreprises perçoivent la gouvernance des données comme un actif opérationnel, un actif stratégique ou une question d'ordre réglementaire et juridique. Nous avons également étudié l'intégration de la gouvernance des données dans trois pratiques financières : l'utilisation de KPI établissant un lien entre la gouvernance des données et la performance financière, la prise en compte de la protection des données dans le reporting financier et l'intégration des risques liés aux données dans les valorisations financières. Nous avons constaté que les entreprises qui ont une vision stratégique de la gouvernance sont davantage susceptibles d'intégrer la gouvernance des données dans leurs pratiques concrètes.

À partir de la question à choix multiples portant sur la perception de la conformité, les répondants ont été répartis en deux groupes : ceux ayant sélectionné « actif stratégique / avantage concurrentiel » (vision stratégique) et ceux ayant sélectionné « actif opérationnel » ou « question réglementaire et juridique » (vision opérationnelle). Nous avons ensuite comparé l'adoption de trois pratiques financières entre ces deux groupes : disposer de KPI établissant un lien entre la gouvernance des données et la performance (au moins un KPI indiqué comme « oui »), publier un reporting quantitatif sur les données

et prendre en compte les risques liés aux données dans les évaluations (notation financière, bilan, flux de trésorerie futurs ou opérations de fusion-acquisition passées). Chaque comparaison porte uniquement sur les répondants ayant répondu à la fois à la question sur la perception et à la question portant sur la pratique concernée. Le lien est mesuré au moyen d'un odds ratio (via une régression logistique), complété par un test du khi-deux. **Les entreprises qui perçoivent la conformité comme un actif sont davantage susceptibles de mettre en œuvre chacune de ces pratiques** : 49 % des entreprises qui considèrent la gouvernance des données comme un actif stratégique utilisent également des KPI établissant un lien entre la gouvernance des données et la performance, contre 25 % des organisations qui considèrent la gouvernance des données comme un actif opérationnel ou une question réglementaire et juridique ; 21 % intègrent quantitativement la gouvernance des données dans leur reporting, contre 8 % ; et 24 % intègrent les risques liés aux données dans leurs valorisations, contre 10 %. Les odds ratios se situent entre 2,8 et 3,1 pour les trois modalités ($p < 0,01$). Cet effet ne s'explique pas uniquement par un biais lié à la taille des entreprises : après prise en compte de la taille et du secteur d'activité dans la régression logistique, il demeure significatif pour les trois pratiques.

À partir de la question 4 (niveau auquel la réponse a été formulée), nous avons comparé les réponses fournies « au niveau de la direction financière du groupe » ($n = 40$) à l'ensemble des autres réponses, selon les trois pratiques d'intégration financière. Les réponses formulées au niveau de la direction financière du groupe ne semblent pas être associées à une adoption plus importante de l'une ou l'autre de ces pratiques : KPI données-performance de la question 12 (32,5 % contre 34,9 %, $p = 0,85$), bases de données reflétées dans les états financiers de la question 15 (30,0 % contre 30,9 %) et risque lié aux données pris en compte dans l'évaluation de la question 16 (20,0 % contre 13,3 %, avec un odds ratio de 1,62 mais non significatif, $p = 0,32$).

3.4. Reporting extra-financier

« Dans quelle mesure vos auditeurs intègrent-ils la protection des données et la conformité dans leur audit annuel de vos contrôles internes et de vos risques financiers ? »

Le niveau de détail publié sur la protection des données reste faible pour une grande partie de l'échantillon. 38 % des entreprises n'abordent pas le sujet dans leurs rapports annuels extra-financiers, et 22 % se limitent à une mention minimale, une simple déclaration de conformité. Des efforts de communication existent, principalement qualitatifs (description des politiques internes, rôle du DPO, actions de formation) pour 34 %, tandis que la communication quantitative (volume de demandes d'exercice des droits des personnes, montants investis dans la cybersécurité, mesure chiffrée de l'exposition aux risques) ne concerne que 13 % des entreprises.

3.5 Place de la protection des données dans les audits et les contrôles

Nous avons également interrogé les entreprises sur leurs pratiques d'audit concernant leurs données. Nous constatons que la pratique la plus répandue consiste à examiner les éléments informatiques de base sans réaliser d'audit de conformité au RGPD (46 %), suivie du fait d'interroger le DPO ou le service juridique sur l'existence de sanctions réglementaires ou de procédures judiciaires en cours (30 %). Nous avons également observé des pratiques intégrant la protection des données dans les audits, telles que le recours à des spécialistes de la cybersécurité ou des systèmes d'information en complément des auditeurs financiers (21 %), la mise à disposition de documents d'audit dédiés à la protection des données et à la cybersécurité (19 %) et la vérification des bases de données générant des revenus afin de s'assurer de leur conformité au RGPD (15 %).

Un rapprochement mérite tout particulièrement d'être souligné : lorsque la protection des données et la cybersécurité sont jugées critiques et font l'objet d'un document d'audit dédié, les risques liés aux données sont bien plus fréquemment intégrés dans diverses formes d'évaluation (question 18). Parmi les 189 répondants ayant répondu aux deux questions, 33 % des entreprises ayant fourni un document d'audit dédié à la protection des données et à la cybersécurité intègrent également les risques liés aux données dans leurs valorisations, contre 11 % des entreprises n'ayant pas fourni de document d'audit dédié. Le test de Fisher donne un odds ratio de 3,96 ($p = 0,0033$), avec un intervalle de confiance à 95 % compris entre 1,52 et 10,15. Cet intervalle est relativement large en raison de la faible taille des échantillons.

Nous avons demandé aux entreprises ayant participé à des opérations de fusion-acquisition (76 répondants) comment elles avaient audité les bases de données acquises dans le cadre du processus de due diligence. Près des deux tiers (63 %) indiquent que celles-ci avaient été examinées dans le cadre de l'audit juridique et informatique général. 25 % ont réalisé une « due diligence » spécifiquement consacrée à la valeur des bases de données ou à leur conformité, tandis que **18 % ont réalisé la « due diligence » accompagnée de l'élaboration d'une feuille de route détaillée en matière de conformité**. Environ 13 % des répondants ont sélectionné la réponse « Autre ».

Nous avons demandé aux organisations comment elles intègrent la protection des données, la cybersécurité et l'IA dans leurs stratégies ESG (environnementales, sociales et de gouvernance) plus larges. De loin, la réponse la plus fréquente était la suppression des données obsolètes, qui permet également de réduire la consommation énergétique des serveurs et l'empreinte carbone numérique (70 %), une approche qui peut nécessiter peu d'efforts. Les entreprises mettent également en œuvre des pratiques plus exigeantes, notamment en appliquant des critères ESG à la sélection de leurs fournisseurs de technologies (21 %), en communiquant publiquement sur leurs pratiques en matière de protection des données (20 %), en mettant en place un comité d'éthique chargé de l'utilisation des données sensibles à des fins de monétisation des données (13 %), en publiant des indicateurs clés de performance (KPI) liés aux données (10 %) et en auditant les algorithmes afin d'identifier les biais et les discriminations (9 %). La part importante de réponses « autres » (21 %) laisse penser que de nombreuses entreprises ont peut-être développé

d'autres approches adaptées à leurs modèles économiques ou ne disposent pas encore d'un cadre clairement établi.

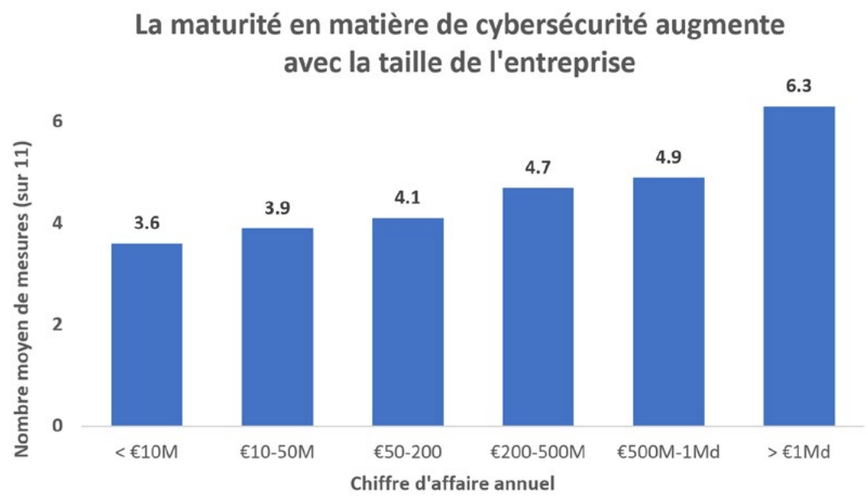
3.6. Transparence financière pour les sociétés cotées

Ces deux dernières questions demandaient aux répondants d'indiquer, sur une échelle de 1 à 5, si la protection des données devrait se refléter dans la valeur de marché d'une entreprise et si une gouvernance exemplaire des données devrait améliorer les conditions de financement. Ces questions n'ont été renseignées que par 19 et 18 répondants, de sorte que les résultats sont indicatifs et ne peuvent être généralisés.

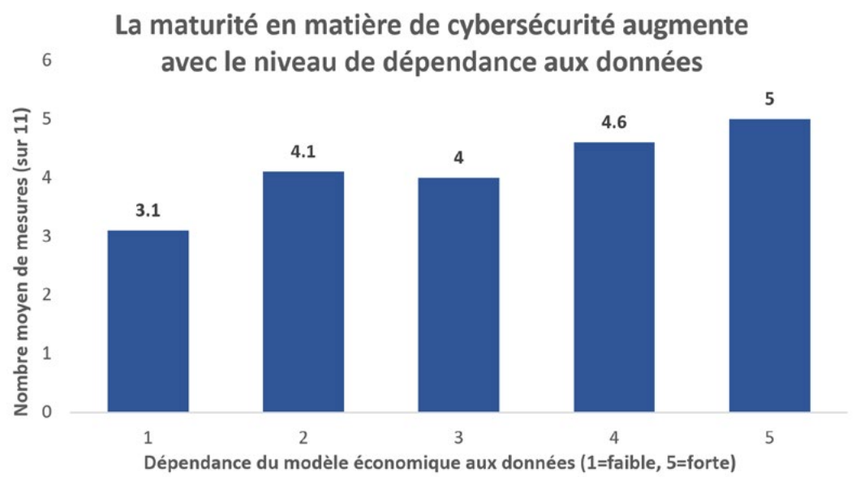
L'adhésion est modérée mais nettement positive (moyenne de 3,6/5) : la moitié des répondants sont d'accord ou tout à fait d'accord pour dire que la protection des données devrait se refléter dans la valeur de marché, presque aucun n'est en désaccord et les autres restent indécis. S'agissant des conditions de financement, les réponses sont plus réservées (moyenne de 3,1/5) : près de la moitié restent neutres et environ un quart sont même en désaccord avec l'idée qu'une gouvernance exemplaire se traduise par de meilleures conditions de financement.

4. Enjeux de cybersécurité

Nous avons interrogé les organisations sur les actions, les pratiques d'audit et de certification qu'elles ont mises en œuvre au cours des cinq dernières années en matière de protection des données et de cybersécurité. La formation des collaborateurs est pratiquement généralisée (88,5 %), suivie de près par la mise à jour annuelle des politiques internes de confidentialité et des directives destinées aux collaborateurs (73 %), les simulations de phishing (68,5 %) et les tests d'intrusion sur les systèmes critiques (60,5 %). Ces quatre mesures sont adoptées par une nette majorité des entreprises, y compris les plus petites : même les entreprises réalisant moins de 10 M€ de chiffre d'affaires mettent en œuvre en moyenne 3,6 des 11 mesures proposées. Parmi les autres pratiques déjà mises en place par les entreprises figurent notamment les certifications telles que la norme ISO 27001 (27,5 %), les audits de conformité des fournisseurs critiques (22,5 %), le reporting formalisé et quantifié en matière de cybersécurité (21 %), les analyses d'impact relatives à la protection des données (AIPD) systématiques (37 %) et la certification RGPD (16 %). Les pratiques les moins répandues sont la cartographie automatisée des flux de données (11,5 %) et les programmes de signalement des vulnérabilités (7 %).



Graphique 13 Taille des entreprises et adoption des pratiques de cybersécurité



Graphique 14 Dépendance des entreprises aux données et adoption des pratiques de cybersécurité

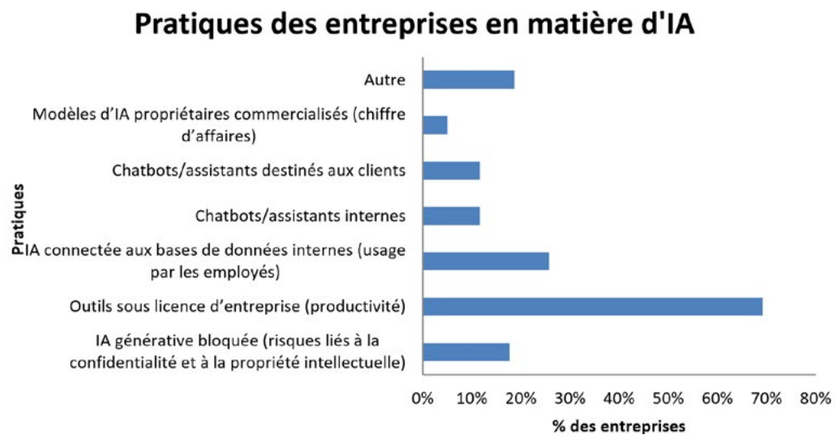
Grâce à une analyse croisée, nous constatons que le niveau de maturité augmente significativement avec la taille de l'entreprise (de 3,6 mesures pour les plus petites à 6,3 pour les plus grandes), ce qui indique que l'application de ces pratiques est probablement amenée à progresser à mesure que la taille de l'entreprise, et donc ses ressources, augmente. Le nombre moyen de pratiques de cybersécurité mises en œuvre augmente également avec le niveau de dépendance aux données déclaré : il passe de 3,1 mesures (sur 11) pour les entreprises les moins dépendantes à 5,0 pour les plus dépendantes. Cette relation est statistiquement significative, mais d'intensité modérée : la corrélation de Spearman est de 0,23 ($p = 0{,}001$) et une régression de Poisson indique que chaque point supplémentaire de dépendance augmente d'environ 10 % le nombre attendu de mesures (IRR = 1,10 ; IC à 95 % : 1,04–1,16 ; $p < 0{,}001$).

Les entreprises cherchent déjà à quantifier le coût d'une cyberattaque majeure : 40 % s'appuient sur une estimation approximative (moyennes sectorielles, police d'assurance cyber), 12 % calculent les coûts directs, et 18 % vont jusqu'à intégrer les pertes indirectes, ce qui constitue la pratique la plus avancée. Par ailleurs, 30 % considèrent les incidents cyber comme un problème informatique et ne disposent d'aucun processus permettant d'évaluer le coût d'un incident cyber.

Selon les réponses en texte libre, plusieurs entreprises fondent leur quantification sur des méthodes structurées : analyses de risques EBIOS-RM croisant probabilité et gravité, modèles internes au niveau du groupe intégrant les coûts directs, les interruptions d'activité et les responsabilités potentielles, ou encore une estimation établie « à partir des coûts de restauration du SI, des prestations de cybersécurité et des interruptions d'activité ». D'autres utilisent le calcul des primes d'assurance cyber comme méthode d'estimation du risque, ou en l'intégrant à la cartographie annuelle des risques revue au niveau du groupe. Enfin, de nombreuses réponses témoignent davantage d'une démarche en cours plutôt que d'une absence de dispositif : « estimation prévue pour l'année », « démarche en cours au niveau du groupe : plan d'action cybersécurité NIS 2 », « dispositif actuellement en cours de mise en place à la suite du carve-out, avec la nomination d'un responsable de la sécurité (CSO) ».

En matière de communication des sociétés cotées (18 réponses seulement), les résultats sont à lire avec prudence. La stratégie privilégiée consiste à attendre les résultats de l'enquête technique avant de communiquer ou à informer sur les activités touchées, plutôt qu'à communiquer par exemple un chiffre de perte maximale.

5. Pratiques en matière d'IA



Graphique 15 Pratiques des entreprises en matière d'IA

Plus des deux tiers des entreprises (69 %) utilisent déjà des outils sous licence entreprise pour gagner en productivité, l'IA est donc entrée dans le quotidien professionnel.
18 % bloquent délibérément l'IA générative grand public pour des raisons de confidentialité et de propriété intellectuelle. Un quart des répondants (26 %) connectent l'IA à leurs bases de données internes, et 11,6 % déploient des chatbots ou des assistants, internes ou destinés aux clients. 5 % commercialisent des modèles d'IA propriétaires générateurs de revenus. L'adoption des outils d'IA est généralisée, mais les niveaux d'intégration ou de maîtrise varient fortement d'une entreprise à l'autre.

Plusieurs entreprises développent leurs propres outils « à partir de solutions d'IA existantes avec anonymisation et filtrage des données », ou déploient une « version personnalisée et sécurisée de Copilot selon un cahier des charges » ainsi qu'un système d'IA juridique fermé, à accès restreint. Les règles d'utilisation sont également formalisées. Certaines entreprises mettent en place des chartes relatives à l'IA, des « lignes directrices encadrant l'utilisation de l'IA », des programmes pilotes ouverts à un nombre limité de collaborateurs avant un déploiement à grande échelle, ou encore le blocage ciblé des outils considérés comme problématiques. L'utilisation de ces outils dans les activités professionnelles comprend notamment l'évaluation des déclarations de sinistres pour appuyer la prise de décision des experts dans le secteur de l'assurance, l'aide à la recherche et à l'analyse de cibles d'investissement, ou en encore la mise à disposition solutions de calcul haute performance (HPC) aux clients pour leurs applications d'IA.

En mettant en relation les résultats concernant les pratiques en matière d'IA avec d'autres variables, nous pouvons dégager des enseignements intéressants. Le nombre de pratiques adoptées semble augmenter avec la taille de l'entreprise (en termes de chiffre d'affaires). À l'aide d'un modèle de régression de Poisson (avec un rapport déviance/degrés de liberté de 0,81), nous constatons que chaque tranche de chiffre d'affaires (5-10

M€, 10-50 M€, 50-200 M€, 200-500 M€, 500 M€-1 Md€ et plus de 1 Md€) est associée à une augmentation d'environ 17 % du nombre de pratiques en matière d'IA (IRR = 1,17 ; IC : 1,08–1,27 ; p = 0,0001). À l'instar des pratiques en matière de cybersécurité, l'adoption de l'IA semble augmenter avec la taille de l'entreprise et, par conséquent, avec ses ressources.

Le nombre de pratiques en matière d'IA est également corrélé de manière positive et significative à la maturité en cybersécurité (coefficient de Spearman de 0,36, p < 0,001). Cela suggère que **l'adoption de l'IA va de pair avec la maturité en cybersécurité**.

Les entreprises utilisant des applications d'IA avancées (telles que des systèmes d'IA connectés aux bases de données internes, des chatbots destinés aux clients ou des modèles d'IA commercialisés) sont davantage susceptibles de prendre en compte les risques liés aux données dans l'une des évaluations financières (question 16), avec notamment 24 % contre 10 % (odds ratio de 2,67 ; p = 0,020). Autrement dit, les résultats indiquent que lorsque l'IA génère de la valeur à partir des données, les entreprises commencent à prendre en compte les risques associés en termes financiers. Cela met en évidence un lien notable entre l'utilisation de l'IA et le reporting financier. Nous n'avons en revanche pas constaté de corrélation significative entre la valeur déclarée de la dépendance aux données et le nombre de pratiques en matière d'IA mises en œuvre, contrairement à ce que nous avons observé pour les mesures de cybersécurité.

6. Enquête menée auprès d'entreprises luxembourgeoises

Dans le cadre de l'étude conjointe menée par la CNPD, la CNIL et l'ICO, un questionnaire a été adressé à une sélection d'entreprises établies au Luxembourg afin d'évaluer la manière dont les enjeux de protection des données, de cybersécurité et d'intelligence artificielle sont intégrés dans les stratégies financières, les processus de gouvernance et, plus largement, dans l'évaluation des entreprises. L'échantillon luxembourgeois a enregistré un taux de réponse de 30 %.

Les entreprises qui ont répondu sont majoritairement de grandes organisations. Ainsi, 83 % déclarent un chiffre d'affaires supérieur à 200 millions d'euros, et deux tiers des participants emploient plus de 1 000 salariés. Par ailleurs, un tiers des répondants relèvent des secteurs de la finance et de l'assurance.

La plupart des participants indiquent traiter des données à caractère personnel courantes (près de 90 %), tandis que 50 % déclarent traiter des données sensibles. A l'inverse, le traitement de données de profilage ou comportementales reste plus limité (environ 22 %). En matière de gouvernance, les résultats indiquent un niveau de maturité relativement élevé : 56 % des organisations ont mis en place des indicateurs de performance des données liés aux résultats financiers. 83 % réalisent systématiquement des analyses d'impact relatives à la protection des données (AIPD) et 67 % disposent d'un dispositif de reporting chiffré sur le risque cyber. À l'inverse, seul un tiers des entreprises déclarent exiger des audits de conformité de la part de leurs prestataires tiers critiques.

Malgré une maturité croissante en matière de gouvernance des données, **l'intégration des données dans les systèmes comptables semble encore balbutiante** dans de nombreuses organisations. 28 % des entreprises indiquent que les coûts de développement de logiciels et de bases de données sont immobilisés au bilan en tant qu'immobilisations incorporelles. À l'inverse, près des deux tiers des répondants déclarent soit ne pas savoir comment les données sont comptabilisées (39 %), soit qu'elles ne font l'objet d'aucun traitement comptable identifiable (28 %).

S'agissant des pratiques en matière d'intelligence artificielle, les entreprises établies au Luxembourg ont d'ores et déjà largement recours aux outils d'IA. Près de 78 % déclarent utiliser des solutions d'IA sous licence professionnelle. Par ailleurs, 22 % connectent ces outils à leurs bases de données internes, 28 % des organisations interrogées ont mis en place des chatbots en contact direct avec les clients, tandis que 22 % ont choisi de bloquer les outils d'IA générative grand public afin de limiter les risques en matière de confidentialité ou de propriété intellectuelle. Ces résultats suggèrent que l'intelligence artificielle s'impose progressivement comme un outil de productivité au sein des organisations.

Les deux questions d'opinion du questionnaire révèlent une vision prudente du lien entre protection des données et création de valeur. Lorsqu'il leur a été demandé si la protection des données devait se refléter dans la valeur de marché des entreprises, les organisations interrogées ont exprimé des positions plutôt conservatrices, 89 % étant tout à fait en désaccord. De même, l'idée selon laquelle une gouvernance exemplaire des données pourrait conduire à des conditions de financement plus favorables n'a recueilli qu'un soutien modéré, avec une note moyenne de 2,7 sur 5. Cette perception suggère que, pour cet échantillon d'entreprises, les enjeux liés à la protection des données sont encore principalement considérés sous l'angle de la conformité et de la gestion des risques, plutôt que comme un levier de création de valeur financière.

Bien que les entreprises interrogées présentent un niveau de maturité élevé en matière de gestion et de protection des données, l'évaluation économique de ces actifs n'en est encore qu'à ses débuts. Les résultats suggèrent un potentiel important de développement des pratiques comptables et financières, afin que les données, déjà reconnues comme un enjeu de gouvernance, puissent progressivement être considérées comme un véritable levier de création de valeur.

7. Annexe : Réponses complètes au questionnaire pour la France

À noter que, parmi les 204 formulaires soumis, 2 entreprises n'ont donné aucune réponse.

Combien de salariés compte l'entreprise ? 200 répondants

- moins de 50 salariés : 38
- entre 50 et 200 salariés : 64
- entre 200 et 1 000 salariés : 56
- entre 1 000 et 5 000 salariés : 25
- plus de 5 000 salariés : 18

2. Quel est le chiffre d'affaires annuel approximatif de votre entreprise ? 200 répondants

- moins de 10 M€ : 32
- entre 10 M€ et 50 M€ : 62
- entre 50 M€ et 200 M€ : 53
- entre 200 M€ et 500 M€ : 22
- entre 500 M€ et 1 Md€ : 13
- plus de 1 Md€ : 19

3. Dans quelle région votre siège social est-il situé ? 197 répondants

- Auvergne-Rhône-Alpes : 25
- Bourgogne-Franche-Comté : 4
- Bretagne : 10
- Centre-Val de Loire : 2
- Corse : 3
- Grand Est : 11
- Hauts-de-France : 8
- Île-de-France : 68
- Normandie : 7
- Nouvelle-Aquitaine : 15
- Occitanie : 12
- Pays de la Loire : 15
- Provence-Alpes-Côte d'Azur : 12
- Martinique : 3
- La Réunion : 2

Si votre entreprise fait partie d'un groupe, précisez si votre réponse – 194 répondants

- est faite au niveau de la direction financière du groupe, afin de refléter les enjeux de consolidation comptable et de reporting : 40
- est faite au niveau de votre entreprise, pour des raisons tenant à la nature de votre activité ou à votre structure financière, et précisez lesquelles : 60
- si vous êtes le DPO du groupe, cochez cette case : 79
- non concerné : 62

5. Quelle est la structure financière de votre entreprise et son niveau d'exposition aux marchés financiers ? 198 répondants

- cotation en bourse : actions négociées sur un marché réglementé : 21
- émetteur d'obligations ou d'autres titres de créance notés par des agences de notation : 7
- une partie de votre capital est détenue par des investisseurs financiers professionnels (capital-risque, capital-investissement / LBO, fonds institutionnels) : 46
- aucune des propositions ci-dessus : 135

6. Votre entreprise a-t-elle déjà réalisé une opération de croissance externe au cours des cinq dernières années ? (fusion/acquisition…) 199 répondants

- oui, en tant que cédant : 22
- oui, en tant qu'acquéreur : 73
- non : 117

7. Quel est votre principal secteur d'activité ? 197 répondants

- Agriculture, sylviculture et pêche : 3
- Industries extractives : 1
- Industrie manufacturière : 32
- Production et distribution d'électricité, de gaz, de vapeur et d'air conditionné : 2
- Production et distribution d'eau ; assainissement, gestion des déchets et dépollution : 2
- Construction : 4
- Commerce ; réparation d'automobiles et de motocycles : 20
- Transports et entreposage : 16
- Hébergement et restauration : 1
- Information et communication : 14
- Activités financières et d'assurance : 21
- Activités immobilières : 3
- Activités spécialisées, scientifiques et techniques : 5
- Activités de services administratifs et de soutien : 15
- Administration publique : 4
- Enseignement : 1
- Santé humaine et action sociale : 2
- Arts, spectacles et activités récréatives : 1
- Autres activités de services : 50

8. Comment évalueriez-vous la dépendance de votre modèle économique au traitement de données ? (Remarque : les options n'ont pas de libellé explicite dans le rapport, seulement une échelle numérotée de 1 à 5) 199 répondants

- Option 1 : 21
- Option 2 : 38
- Option 3 : 51
- Option 4 : 52
- Option 5 : 37

9. Comment classeriez-vous les données traitées par votre organisation ? 200 répondants

- informations B2C courantes (fichier clients, etc.) : 143
- comportement et profilage : 33
- données sensibles : 75
- autre (précisez votre réponse ci-dessous) : 53

10. Quels types d'intelligence artificielle sont actuellement déployés au sein de votre organisation, et comment interagissent-ils avec vos données ? 198 répondants

- les outils d'IA générative sont bloqués sur nos réseaux en raison des risques liés à la confidentialité des données / à la propriété intellectuelle : 35
- vous utilisez des outils sous licence entreprise pour optimiser votre productivité interne : 137
- vous connectez l'IA à vos bases de données internes, exclusivement réservée à l'usage de vos salariés : 51
- nous déployons / vous déployez des chatbots ou des assistants automatisés qui interagissent directement avec nos/vos clients : 23
- vous commercialisez des modèles d'IA propriétaires ou des analyses générées par l'IA, qui constituent une source directe de revenus : 10
- autre (précisez votre réponse ci-dessous) : 37

11. Comment la conformité et la gouvernance des données sont-elles principalement perçues au sein de votre comité exécutif / conseil d'administration ? 200 répondants

- comme un enjeu réglementaire et juridique : 166
- comme un facteur opérationnel nécessaire (protection de la réputation) : 115
- comme un actif stratégique et un possible avantage concurrentiel : 69
- autre (précisez votre réponse ci-dessous) : 11

Avez-vous mis en place des indicateurs clés de performance (KPI) spécifiques reliant la gouvernance des données et la performance financière ? 199 répondants

- non : 130
- oui, reflétant les risques (nombre de violations de données, etc.) : 48
- oui, orientés protection des clients / commercial : 21
- oui, nous utilisons des KPI financiers liés aux données (précisez si possible) : 12
- autre (précisez votre réponse ci-dessous) : 7

Parmi les actions, audits ou certifications suivants, lesquels ont été mis en œuvre au sein de votre organisation au cours des 5 dernières années en matière de protection des données et de cybersécurité ? 200 répondants

- mise à jour annuelle des politiques internes de confidentialité et des consignes destinées aux salariés : 146
- formation des salariés : 177
- réalisation systématique d'analyses d'impact relatives à la protection des données (AIPD) : 74
- simulations d'hameçonnage : 137
- tests d'intrusion sur les systèmes critiques : 121
- utilisation d'un logiciel automatisé pour cartographier et classer en continu les flux de données sensibles : 23
- programmes permanents de divulgation des vulnérabilités ouverts à des chercheurs externes : 14
- rapports formalisés et chiffrés sur les risques cyber et liés aux données : 42
- certifications auditées par un organisme externe (ISO 27001…) : 55
- audits de conformité imposés à tous les fournisseurs tiers critiques : 45
- certification RGPD : 32
- autre (précisez votre réponse ci-dessous) : 17

14. Votre organisation a-t-elle estimé le coût potentiel d'une cyberattaque ou d'une fuite de données majeure ? 191 répondants

- vous considérez le risque cyber principalement comme un problème informatique et ne disposez pas de processus pour estimer le coût d'un incident majeur pour l'entreprise : 58
- estimation approximative fondée sur des moyennes sectorielles ou utilisation du plafond de garantie de votre assurance cyber comme estimation de référence : 77
- vous avez calculé les coûts directs d'un incident (restauration du système informatique, etc.) : 23
- vous avez calculé à la fois les coûts directs et les pertes indirectes (coût horaire de l'indisponibilité, perte de chiffre d'affaires, etc.) : 34
- vous modélisez ces risques à l'aide de l'intelligence artificielle : 2
- autre (précisez votre réponse ci-dessous) : 31

15. Comment vos bases de données sont-elles principalement reflétées dans vos états financiers ? 199 répondants

- pas du tout : 76

- coûts de développement informatique et de logiciels de bases de données, en tant qu'immobilisation incorporelle au bilan : 55
- en tant qu'actif inclus dans le goodwill (si une opération d'acquisition a eu lieu) : 10
- vous ne savez pas : 58
- autre (précisez votre réponse ci-dessous) : 7

À votre connaissance, comment les risques liés aux données sont-ils principalement pris en compte dans l'évaluation financière de votre entreprise, que ce soit en interne ou par des acteurs externes ? 196 répondants

- non pris en compte : 102
- pris en compte lors d'une opération de fusion-acquisition passée : 16
- pris en compte, à votre connaissance, dans votre notation financière : 8
- pris en compte au bilan en tant qu'immobilisation incorporelle dans le goodwill : 6
- reflétés par des ajustements des flux de revenus futurs ou du coût du capital que vous utilisez (méthode DCF) : 2
- vous ne savez pas : 64
- autre (précisez) : 8

17. Quel niveau de détail concernant la protection des données figure dans vos rapports annuels extra-financiers ? (le cas échéant) 193 répondants

- non abordé : 74
- minimal (simple déclaration de conformité légale) : 42
- qualitatif (description des politiques, présence d'un DPO, programmes de formation) : 65
- quantitatif (nombre de demandes, investissements en cybersécurité, exposition chiffrée aux risques…) : 25
- autre (précisez votre réponse ci-dessous) : 19

18. Dans quelle mesure vos auditeurs intègrent-ils la protection des données et la conformité dans leur audit annuel de vos contrôles internes et de vos risques financiers ? 192 répondants

- ils examinent également des éléments informatiques de base, mais n'auditent pas la conformité au RGPD : 88
- ils interrogent le DPO / l'équipe juridique pour identifier les sanctions réglementaires ou contentieux en cours : 57
- le cabinet d'audit fait appel à des spécialistes de la cybersécurité et de l'informatique, en

complément des auditeurs financiers, pour tester notre infrastructure de données : 41

- ils vérifient que les bases de données générant vos principaux revenus sont conformes au RGPD : 29
- la protection des données et la cybersécurité sont considérées comme critiques et font l'objet d'un document d'audit dédié : 37
- autre (précisez ci-dessous) : 30

Comment votre organisation intègre-t-elle concrètement la protection des données, la cybersécurité et l'IA dans sa stratégie ESG (environnementale, sociale et de gouvernance) globale ? 184 répondants

- vous supprimez les données clients obsolètes, ce qui réduit également la consommation d'énergie de vos serveurs et votre empreinte carbone numérique : 128
- vous publiez des rapports sur vos efforts de protection des données de vos clients et de vos salariés : 36
- vous réalisez des audits de vos algorithmes afin de prévenir toute discrimination, tout biais et toute inégalité d'accès aux données : 16
- vous disposez d'un comité d'éthique dédié qui se prononce sur les projets sensibles de monétisation des données et de déploiement de l'IA : 24
- vous appliquez des critères ESG stricts lors de la sélection de vos fournisseurs de technologies et courtiers en données : 39
- vous publiez un rapport détaillant des indicateurs clés de performance (KPI) relatifs aux données des utilisateurs et à votre niveau global de cybersécurité : 18
- autre (précisez votre réponse ci-dessous) : 39

S'agissant du processus de due diligence : lors de l'acquisition d'une société cible, comment la conformité des données/bases de données a-t-elle été auditée ? 76 répondants

- couverture de premier niveau dans le cadre de l'audit juridique/informatique général : 48
- dans le cadre d'une « due diligence » portant sur la valeur des bases de données ou leur conformité : 19
- dans le cadre d'une « due diligence » portant sur la valeur des bases de données ou les questions de conformité, avec une feuille de route détaillée de mise en conformité : 14
- autre (précisez votre réponse si possible) : 10

21. Le cas échéant, lors de vos précédentes opérations de fusion-acquisition, la découverte de données non conformes a-t-elle eu des conséquences financières directes ? 67 répondants

- non / aucun impact : 33
- exigence de garanties de passif spécifiques : 13
- révision à la baisse du prix d'acquisition : 3
- annulation d'une opération : 2
- autre (précisez votre réponse ci-dessous) : 20

22. Lors l'intégration comptable, comment les bases de données clients acquises ont-elles été valorisées ? 72 répondants

- aucune valorisation : 38
- elles ont été entièrement intégrées au goodwill (sans être isolées) : 10
- elles ont été isolées et valorisées au bilan en tant qu'immobilisations incorporelles spécifiques : 13
- autre (précisez votre réponse ci-dessous) : 11

La protection des données sur les marchés financiers devrait être reflétée de manière transparente, par exemple dans l'évaluation des entreprises ou dans d'autres rapports financiers. 19 répondants

- Option 1 : 0
- Option 2 : 1
- Option 3 : 8
- Option 4 : 7
- Option 5 : 3

.Une gouvernance exemplaire des données permet aux entreprises d'obtenir des conditions de financement plus favorables (baisse du coût de la dette / des fonds propres, amélioration de la notation, impact sur le WACC ou coût moyen pondéré du capital). 18 répondants

- Option 1 : 2
- Option 2 : 3
- Option 3 : 8
- Option 4 : 2
- Option 5 : 3

25. En cas d'incident de cybersécurité ou de fuite de données majeure, quelle est votre principale

stratégie de communication financière pour limiter la volatilité boursière à court terme ? 17 répondants

- attendre les résultats complets de l'enquête technique avant de communiquer auprès du marché : 7
- communiquer immédiatement pour confirmer quelles activités/données essentielles ne sont pas touchées : 6
- communiquer immédiatement un chiffre précis des pertes financières maximales afin de lever l'incertitude du marché : 2
- autre (précisez la réponse ci-dessous) : 3

B. Exemple pratique : regroupement d'entreprises portant sur une base de données clients (IFRS 3, IAS 38 et IAS 36)

Dans le cadre d'un regroupement d'entreprises, l'interaction entre IFRS 3, IAS 38 et IAS 36 peut être illustrée par l'acquisition d'une société dont la valeur provient principalement de ses données clients et de ses capacités d'analyse.

Supposons qu'une société A, établie dans l'UE, acquière la société B pour un prix d'acquisition de 20 000 000 EUR. Conformément à IFRS 3, les actifs identifiables et les passifs sont comptabilisés aux valeurs suivantes[36] :

Base de données clients : 3 000 000 EUR

Relations clients : 2 000 000 EUR

Actifs technologiques : 1 500 000 EUR

Passifs repris : (2 500 000 EUR)

Il en résulte un actif net identifiable de 4 000 000 EUR et la comptabilisation d'un goodwill de 16 000 000 EUR[37], reflétant les synergies attendues et les avantages économiques futurs.

Selon la norme IAS 38, ces immobilisations incorporelles sont comptabilisées séparément et amorties sur leur durée d'utilité. Toutefois, leur valeur économique dépend de la capacité juridique à utiliser les données sous-jacentes. À cet égard, dès lors qu'il s'agit de sociétés établies dans l'Union européenne, la base de données clients doit être conforme au cadre du RGPD. Cela implique notamment, sans que cette liste soit exhaustive, le respect des principes fondamentaux du RGPD énoncés à l'article 5, tels que la licéité, la loyauté, la transparence, la limitation des finalités, la minimisation des données et l'exactitude, ainsi que l'existence d'une base légale valable pour le traitement des données au sens de l'article 6 du RGPD.

L'évaluation financière de l'entreprise est effectuée conformément à la description figurant à la section 3.3.6, selon une approche par actualisation des flux de trésorerie (DCF)[38], conformément à la norme IAS 36 (méthode de la valeur d'utilité). Les principales hypothèses sont les suivantes :

36 Voir le tableau 1. Hypothèses.

37 Voir le tableau 2. IFRS 3 et IAS 38 – Calcul de l'actif net identifiable et du goodwill.

38 Le paragraphe 30 d'IAS 36 définit la valeur d'utilité comme la valeur actualisée des flux de trésorerie futurs, tandis que les paragraphes 33 à 57 énoncent les principes d'estimation et d'actualisation de ces flux.

Période de projection : 5 ans[39]

Taux d'actualisation : 14 %[40]

Taux de croissance à l'infini : 1 %[41]

En l'absence de tout problème réglementaire, les flux de trésorerie prévisionnels passent de 3 000 000 EUR la première année à 4 000 000 EUR la cinquième année[42], reflétant ainsi une évolution stable.

Toutefois, plusieurs mois après l'acquisition, la société A découvre qu'une part importante de la base de données clients a été collectée en violation du RGPD. En conséquence, une partie des données ne peut plus être utilisée à des fins commerciales, ce qui entraîne une diminution des revenus attendus.

À la suite de la découverte de cette non-conformité, les flux de trésorerie prévisionnels sont révisés à la baisse et s'établissent entre 2 000 000 EUR et 2 500 000 EUR sur la période de cinq ans. La valeur terminale est calculée selon la formule de Gordon-Shapiro[43] :

TV[44] $= (CF_5 \times (1 + g)) / (r - g)$

soit une valeur d'environ 19 423 077 EUR[45].

39 La période de projection de cinq ans correspond à la pratique courante en matière de valorisation et est cohérente avec IAS 36, qui limite les prévisions détaillées de flux de trésorerie aux périodes pour lesquelles des estimations fiables peuvent être établies. Au-delà de cet horizon, la performance future est appréhendée au moyen de la valeur terminale.

40 Le taux d'actualisation de 14 % repose sur une estimation simplifiée du coût du capital fondée sur le modèle d'évaluation des actifs financiers (MEDAF). Il se compose d'un taux sans risque d'environ 2,5 %, correspondant au rendement des obligations d'État, et d'une prime de risque de marché d'environ 6 %, ajustée par un bêta sectoriel d'environ 1,5 afin de tenir compte de la volatilité plus élevée des modèles économiques numériques et fondés sur l'exploitation des données. Cette approche conduit à un coût des capitaux propres de base d'environ 11,5 %. Une prime supplémentaire d'environ 2,5 % est ensuite appliquée afin de tenir compte du stade précoce de développement de l'entreprise et de son activité sur un marché très concurrentiel. L'ensemble de ces composantes justifie un taux d'actualisation total d'environ 14 %. Les hypothèses chiffrées retenues sont données à titre indicatif et reposent sur des pratiquent usuelles de modélisation financière. Elles visent à fournir une représentation raisonnable des conditions de marché plutôt qu'une estimation empirique précise.

41 Le taux de croissance à l'infini de 1 % reflète une hypothèse prudente à long terme, globalement cohérente avec les perspectives d'inflation et de croissance des marchés matures des économies développées.

42 Voir le tableau 3. Flux de trésorerie actualisés avant la découverte d'une non-conformité.

43 La valeur terminale est estimée selon le modèle de Gordon-Shapiro (Gordon, 1962), qui repose sur l'hypothèse d'un taux de croissance constant à l'infini. Bien que la norme IAS 36 ne prescrive pas de méthode spécifique pour déterminer la valeur terminale, cette approche est largement utilisée en pratique pour estimer la valeur actuelle des flux de trésorerie générés au-delà de la période de prévision explicite.

44 où : TV = valeur terminale, CF5 = flux de trésorerie de l'année 5, g = taux de croissance à l'infini, r = taux d'actualisation.

45 Voir le tableau 4. Flux de trésorerie actualisés après la perturbation réglementaire.

Sur la base de ces projections révisées, la valeur recouvrable est estimée à environ 17 800 000 EUR. Ce montant étant inférieur à la valeur comptable de 20 000 000 EUR, une perte de valeur d'environ 2 200 000 EUR[46] est comptabilisée, conformément à la norme IAS 36.

Cet exemple illustre la manière dont la norme IFRS 3 encadre la comptabilisation initiale des actifs et du goodwill, dont la norme IAS 38 régit la comptabilisation ultérieure, tandis que la norme IAS 36 veille à ce que les actifs ne soient pas comptabilisés pour un montant supérieur à leur valeur recouvrable lorsque des risques non atténués affectent leur capacité à générer des avantages économiques futurs.

46 Voir le tableau 5. IAS 36 – Calcul de la perte de valeur.

Tableau 1. Hypothèses

Hypothèses	Valeur en EUR
Prix d'acquisition (PP)	20 000 000
Juste valeur de la base de données clients (CD)	3 000 000
Relations clients (CR)	2 000 000
Technologie (T)	1 500 000
Passifs (L)	(2 500 000)
Taux de croissance (GR)	1 %
Taux d'actualisation (DR)	14 %

Tableau 2. IFRS 3 et IAS 38 – Calcul de l'actif net identifiable et du goodwill

Élément	Montant en EUR
Base de données clients (CD)	3 000 000
Relations clients (CR)	2 000 000
Technologie (T)	1 500 000
Passifs (L)	(2 500 000)
Actif net identifiable (NIA) = (CD)+(CR)+(T)+(L)	4 000 000
Goodwill (G) = (PP) – (NIA)	16 000 000

Tableau 3. Flux de trésorerie actualisés avant la non-conformité

Année	Flux de trésorerie en EUR	Taux d'actualisation (DR)	Facteur d'actualisation (DF)	Valeur actualisée (PV1) en EUR
1	3 000 000	14 %	87,72 %	2 631 578,95
2	3 200 000	14 %	76,95 %	2 462 296,09
3	3 500 000	14 %	67,50 %	2 362 400,31
4	3 700 000	14 %	59,21 %	2 190 697,03
5	4 000 000	14 %	51,94 %	2 077 474,66
Valeur terminale (TV)	31 076 923,08	14 %	51,94 %	16 140 380,03
Total des flux de trésorerie				27 864 827,06

Tableau 4. Flux de trésorerie actualisés après la non-conformité

Année	Flux de trésorerie en EUR	Taux d'actualisation (DR)	Facteur d'actualisation (DF)	Valeur actualisée (PV2) en EUR
1	2 000 000	14 %	87,72 %	1 754 385,96
2	2 200 000	14 %	76,95 %	1 692 828,56
3	2 300 000	14 %	67,50 %	1 552 434,49
4	2 400 000	14 %	59,21 %	1 420 992,67
5	2 500 000	14 %	51,94 %	1 298 421,66
Valeur terminale	19 423 076,92	14 %	51,94 %	10 087 737,52
Valeur recouvrable				17 806 800,86

Tableau 5. IAS 36 – Calcul de la perte de valeur et incidence sur les actifs

Élément	Montant en EUR
Valeur comptable (prix d'acquisition)	20 000 000
Valeur recouvrable	17 806 800,86
Perte de valeur	2 193 199,14

Conformément à la norme IAS 36, les pertes de valeur sont comptabilisées dans les états financiers en ramenant la valeur comptable de l'actif à sa valeur recouvrable. Cette exigence garantit que les actifs ne sont pas présentés au bilan pour des montants supérieurs aux avantages économiques attendu de leur utilisation.

Lorsqu'un goodwill est présent, la norme IAS 36 prévoit un mécanisme d'allocation spécifique, selon lequel toute perte de valeur est d'abord imputée sur le goodwill avant d'être affectée aux autres actifs de la même unité génératrice de trésorerie (IAS 36, §§ 59 et 104). Cette disposition reflète le fait que le goodwill constitue une composante résiduelle de la valeur, par nature incertaine, qui intègre souvent des hypothèses relatives aux synergies futures ainsi qu'à des actifs incorporels non identifiables séparément.

D'un point de vue comptable, cela signifie que la perte de valeur n'entraîne pas la comptabilisation d'un actif ou d'un poste distinct. Elle est directement comptabilisée par une diminution de la valeur comptable du goodwill figurant au bilan. Parallèlement, la perte de valeur est comptabilisée en charge dans le compte de résultat, réduisant ainsi le résultat net et, in fine, les capitaux propres.

Ainsi, l'impact financier d'événements défavorables, tels que la diminution de la capacité à utiliser les données clients qui n'ont pas été obtenues de manière conforme à la réglementation, se traduit principalement par une diminution du goodwill comptabilisé dans les états financiers, plutôt que par la création d'un nouveau poste comptable.

C. Parties prenantes consultées

Nous remercions la liste d'organisations suivante d'avoir engagé des discussions avec nous:

- Accountancy Europe
- Association des Banques et Banquiers, Luxembourg (ABBL)
- Bourse de Luxembourg
- Commission de surveillance du secteur financier (Luxembourg)
- E&Y Avocats Paris
- Fédération bancaire française
- Financial Conduct Authority, UK
- HACA Partners Luxembourg
- Haute autorité de l'audit (H2A), France
- S&P Global Ratings
- Seyfarth Shaw LLP

Ainsi que des participants au Data Protection Laboratory du 6 juillet 2026 :

- E&Y Avocats Paris
- Commission de surveillance sur secteur financier (service DPO)
- Fédération bancaire française
- ACO Solutions
- DUSSMAN
- Hôpital Robert Schuman, Luxembourg
- Chatbotaurus
- BGL BNP Paribas
- Stëftung Hëllef Doheem
- HACA Partners

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

ico.