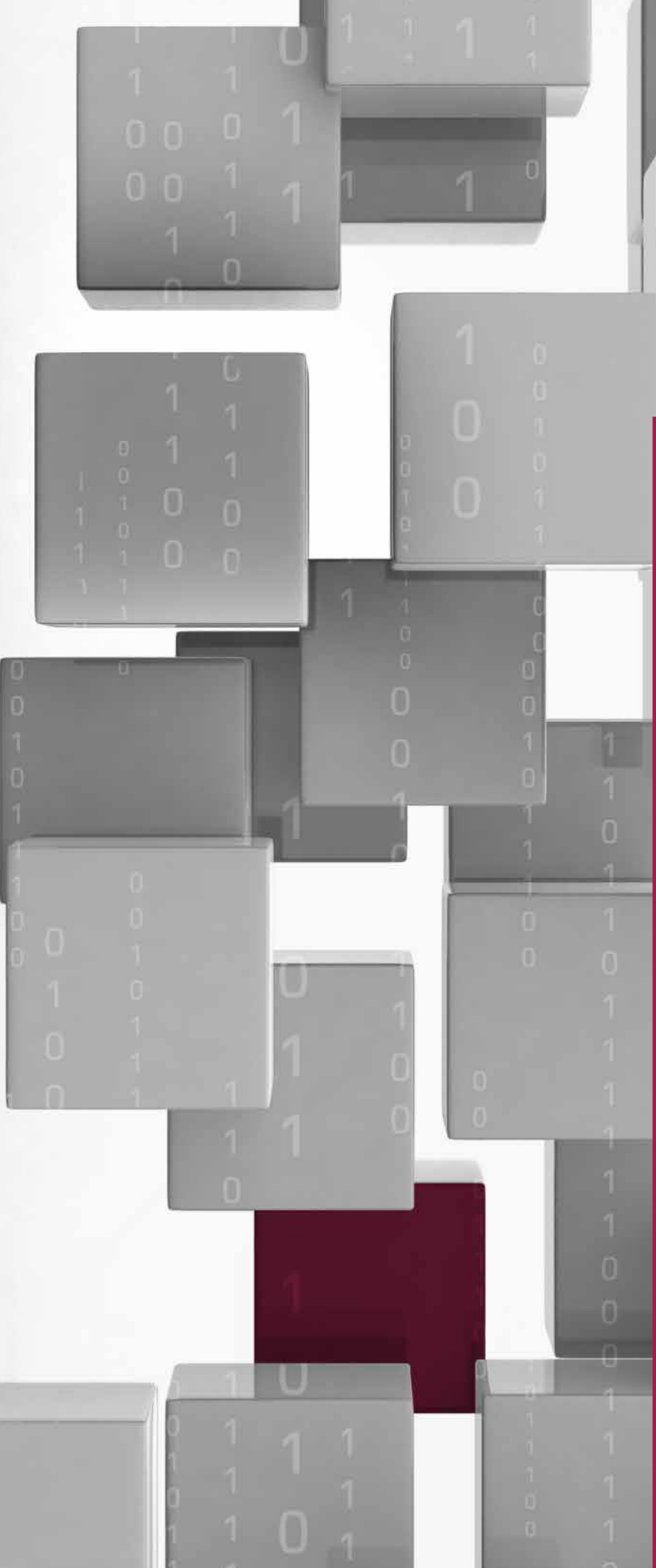


ISACA®
Trust in, and value from, information systems

BIG DATA & PROTECTION DE LA VIE PRIVÉE

LIVRE BLANC DE L'ISACA - AOÛT 2013

Prise de décisions plus éclairées, temps de commercialisation raccourci, service client optimisé et profits accrus, voici quelques-uns des avantages expliquant l'engouement des entreprises de toutes tailles pour la mise en place d'un Big Data. Le Forum économique mondial qualifie les informations personnelles recueillies dans le cadre du Big Data de « nouveau 'pétrole' - une précieuse ressource du 21ème siècle ». L'analytique offerte par le Big Data est le « nouveau moteur de création de valeur économique et sociale ». Avides de récolter les fruits du Big Data et de tirer parti de son vaste potentiel, les entreprises n'en reconnaissent pas moins leur devoir en matière de protection des données personnelles ainsi amassées et analysées. Dans toute initiative liée au Big Data, la gestion des risques et la mise en œuvre de mécanismes adéquats visant à régir et protéger la vie privée doivent plus que jamais être prises en compte. Selon le référentiel COBIT®5 de gouvernance de l'informatique de l'entreprise, permet de maintenir un juste équilibre entre d'un côté, la réalisation de profits, et, de l'autre, l'optimisation des niveaux de risque et l'utilisation des ressources.

ISACA®

Avec plus de 110 000 membres dans 180 pays, l'ISACA *(www.isaca.org)* aide les responsables des activités métier et des technologies de l'information à optimiser la valeur et à gérer les risques liés à l'information et aux technologies. Organisme indépendant à but non lucratif créé en 1969, l'ISACA se veut le défenseur des professionnels de la sécurité de l'information, de l'assurance, de la gestion des risques et de la gouvernance. Pour ces derniers, l'ISACA est une source éprouvée de renseignements dans les domaines des technologies de l'information, des communautés, des normes et de la certification. L'association, qui compte 200 chapitres répartis dans le monde, est par ailleurs à l'origine du progrès et de l'attestation des connaissances et de l'expertise en matière de technologies de l'information par le biais des certifications mondialement reconnues du Certified Information Systems Auditor® (CISA®), du Certified Information Security Manager® (CISM®), du Certified in the Governance of Enterprise IT® (CGEIT®) et du Certified in Risk and Information Systems Control™ (CRISC™). L'ISACA a également développé et met régulièrement à jour COBIT®, un référentiel qui aide les entreprises, quels que soient leur secteur et leur zone géographique, à gérer leurs informations et leurs technologies.

Avertissement

L'ISACA a conçu et créé le livre blanc *Big Data et protection de la vie privée* (le « Document ») principalement comme un élément de formation destiné aux professionnels de la gouvernance et de l'assurance. L'utilisation du présent Document ne constitue en aucun cas une garantie de résultat. Le Document ne saurait être considéré comme incluant l'ensemble des informations, procédures et tests adéquats ou comme excluant d'autres informations, procédures et tests susceptibles de produire raisonnablement des résultats similaires. Pour déterminer si une information, une procédure ou un test spécifique est approprié(e), les professionnels de la gouvernance et de l'assurance doivent se faire leur propre opinion en fonction des cas particuliers rencontrés dans leur environnement technique et informatique spécifique.

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008, États-Unis

Téléphone : +1 847 253 1545

Télécopie : +1 847 253 1443

Courriel : *info@isaca.org*

Site Web : *www.isaca.org*

Faites part de vos commentaires :
www.isaca.org/privacy-and-big-data

Participez au centre de connaissances de l'ISACA :
www.isaca.org/knowledge-center

Suivez l'ISACA sur Twitter :
https://twitter.com/ISACANews

Rejoignez l'ISACA sur LinkedIn : ISACA (site officiel)
http://linkd.in/ISACAOfficial

Aimez l'ISACA sur Facebook :
www.facebook.com/ISACAHQ

Droits d'auteur

REMERCIEMENTS

L'ISACA souhaite remercier :

Équipe de développement de projet

Mario Bojilov
CISA, Meta Business Systems, Australie

Richard Chew
CISA, CISM, CGEIT, Emerald Management Group, États-Unis

Francis Kaitano
CISA, CISM, CEN, Nouvelle-Zélande

Tichaona Zororo
CISA, CISM, CGEIT, CRISC, EGIT, Afrique du Sud

Relecteurs experts

Todd Atteberry
The Atteberry Group, États-Unis

Goutama Bachtiar
Global Innovations and Technology Platform, Indonésie

Graciela Braga
CGEIT, Argentine

Girish Netke
CISA, A-N-G Computer Consultants, Inde

Conseil d'administration de l'ISACA

Tony Hayes
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Gouvernement du Queensland, Australie, Président international

Allan Boardman
CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, Royaume-Uni, Vice-président

Juan Luis Carselle
CISA, CGEIT, CRISC, Wal-Mart, Mexique, Vice-président

Ramses Gallego
CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Espagne, Vice-président

Theresa Grafenstine
CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, Chambre des Représentants, États-Unis, Vice-présidente

Vittal Raj
CISA, CISM, CGEIT, CFE. CIA, CISSP, FCA, Kumar & Raj, Inde, Vice-président

Jeff Spivey
CRISC, CPP, PSP, Security Risk Management Inc., États-Unis, Vice-président

Marc Vael, Ph.D.
CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgique, Vice-président

Gregory T. Grocholski
CISA, The Dow Chemical Co., États-Unis, ancien Président international

Kenneth L. Vander Wal
CISA, CPA, Ernst & Young LLP (retraité), États-Unis, ancien Président international

Christos K. Dimitriadis, Ph.D.
CISA, CISM, CRISC, INTRALOT S.A., Grèce, Directeur

Krysten McCabe
CISA, The Home Depot, États-Unis, Directeur

Jo Stewart-Rattray
CISA, CISM, CGEIT, CRISC, CSEPS, BRM Holdich, Australie, Directeur

Conseil des experts

Christos K. Dimitriadis, Ph.D.
CISA, CISM, CRISC, INTRALOT S.A., Grèce, Président

Rosemary M. Amato
CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., Pays-Bas

Steven A. Babb
CGEIT, CRISC, Betfair, Royaume-Uni

Thomas E. Borton
CISA, CISM, CRISC, CISSP, Cost Plus, États-Unis

Phil J. Lageschulte
CGEIT, CPA, KPMG LLP, États-Unis

Anthony P. Noble
CISA, Viacom, États-Unis

Jamie Pasfield
CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, Royaume-Uni

Comité d'orientation et de pratiques

Phil J. Lageschulte
CGEIT, CPA, KPMG LLP, États-Unis, Président

John Jasinski
CISA, CGEIT, ISO20K, ITIL Exp, SSBB, ITSMBP, États-Unis

Yves Marcel Le Roux
CISM, CISSP, CA Technologies, France

Aureo Monteiro Tavares Da Silva
CISM, CGEIT, Brésil

Jotham Nyamari
CISA, CISSP, Deloitte, États-Unis

James Seaman
CISM, RandomStorm, Royaume-Uni

Gurvinder Singh
CISA, CISM, CRISC, Australie

Siang Jun Julia Yeo
CISA, CPA (Australie), MasterCard Asia/Pacific Pte. Ltd., Singapour

Nikolaos Zacharopoulos
CISA, CISSP, DeutschePost–DHL, Allemagne

Membres et sponsors de l'ISACA et de l'IT Governance Institute® (ITGI®)

Information Security Forum
Institute of Management Accountants Inc.
Les chapitres de l'ISACA
ITGI France
ITGI Japon
Norwich University
Socitum Performance Management Group
Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) de l'Université nationale de Singapour
University of Antwerp Management School

ASIS International
Hewlett-Packard
IBM
Symantec Corp.

Introduction

Le Big Data peut s'avérer particulièrement puissant et avoir un impact à la fois positif et négatif non négligeable sur l'entreprise. **Prise de décisions plus éclairées, temps de commercialisation raccourci, service client optimisé et profits accrus, voici quelques-uns des avantages expliquant l'engouement des entreprises de toutes tailles pour la mise en place d'un Big Data.** Parallèlement à ces avantages, toute faille relative au respect de la vie privée peut avoir des conséquences juridiques financièrement lourdes pour l'entreprise.

Le Big Data a été défini pour la première fois dans un document de Doug Laney[1]. Ce dernier le définit comme des ensembles de données dont les trois caractéristiques principales (volume, vélocité et variété) présentent des défis spécifiques en termes de traitement. La vélocité désigne la vitesse à laquelle les données sont créées, laquelle augmente de manière exponentielle. En 2012, les consommateurs ont dépensé 272 000 USD en achats sur Internet et les marques ont enregistré 34 722 mentions « J'aime » sur leur site Facebook et ce, toutes les minutes. La variété renvoie aux différents types de données traitées. Autrefois simples fichiers et bases de données relationnelles, les données prennent désormais la forme, entre autres, de fichiers audio et vidéo, et d'informations collectées par le biais des capteurs. Le volume est le résultat de l'évolution continue des deux premières caractéristiques, vélocité et variété. Aujourd'hui, les données traitées par les entreprises se chiffrent en téraoctets et en pétaoctets.

Selon la définition donnée par l'ISACA en 2013, le Big Data désigne des ensembles de données qui sont devenus trop volumineux ou qui évoluent trop vite pour être analysés dans un laps de temps raisonnable par le biais des techniques traditionnelles de bases de données multidimensionnelles ou relationnelles, ou encore des outils logiciels habituellement utilisés pour la saisie, la gestion et le traitement des données. « Cette tendance dans le domaine technologique ouvre de nouvelles perspectives en termes de compréhension du monde et de prise de décision dans les entreprises. »[2]

Le Forum économique mondial qualifie les informations personnelles recueillies dans le cadre du Big Data de « nouveau 'pétrole' - une précieuse ressource du 21ème siècle », et son analytique de « nouveau moteur de création de valeur économique et sociale ».[3,4]

Avides de récolter les fruits du Big Data et de tirer parti de son vaste potentiel, les entreprises n'en reconnaissent pas moins leur devoir en matière de protection des données personnelles ainsi amassées et analysées. Dans toute initiative liée au Big Data, la gestion des risques et la mise en œuvre de mécanismes adéquats visant à régir et protéger la vie privée doivent plus que jamais être prises en compte. Selon le référentiel COBIT 5 de gouvernance de l'informatique de l'entreprise, permet de maintenir un juste équilibre entre d'un côté, la réalisation de profits, et, de l'autre, l'optimisation des niveaux de risque et l'utilisation des ressources. Ce référentiel s'applique parfaitement aux défis que pose la protection de la vie privée et à ses exigences.

Le présent livre blanc aborde l'impact du Big Data sur la protection de la vie privée. Il présente les risques, les stratégies et la gouvernance relatifs au respect de la vie privée, ainsi que les éléments à prendre en compte en termes d'assurance.

---

[1] Laney, Doug; « 3D Data Management: Controlling Data Volume, Velocity and Variety », gartner.com, 6 février 2001, *www.blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf*

[2] ISACA.org, « Big Data: Impacts and Benefits », mars 2013, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Big-Data-Impacts-and-Benefits.aspx*

[3] Forum économique mondial, « Personal Data: The Emergence of a New Asset Class », janvier 2011, *www.weforum.org/reports/personal-data-emergence-new-asset-class*

[4] Forum économique mondial, « Unlocking the Value of Personal Data: From Collection to Usage », février 2013, *www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf*

Impacts du Big Data sur la protection de la vie privée

Dans tous les secteurs d'activités (banques, administration, santé, presse, énergie, enseignement, etc.), l'automatisation rapide et continue des processus métiers modifie le paysage de la consommation des données et de leur analyse.

Les entreprises sont en quête d'un retour sur investissement (ROI) acceptable et mesurable dans le domaine du Big Data. À ce titre, les données jusque-là stockées dans des entrepôts en ligne et hors ligne disparates sous une variété de formats, sont désormais disponibles sous forme numérique, prêtes à être corrélées, regroupées et analysées statistiquement en temps réel par groupes entiers de téraoctets et de pétaoctets.

Face à une croissance continue des volumes de données, de leur rapidité de traitement et de leur complexité, et à la multiplication des exigences en termes de protection de la vie privée et de sécurité, les entreprises sont contraintes de trouver de nouvelles réponses aux besoins juridiques, métier et opérationnels.

La décision d'un nombre croissant d'entreprises de transférer leurs données dans le cloud et de recourir aux services d'analyse cloud et aux bases de données analytiques de traitement, telles que les bases de traitement massivement parallèle (MPP) ou de traitement multiprocesseur symétrique (SMP), est largement influencée par le Big Data.

Ce dernier génère un certain nombre de débats sur les lois internationales en matière de protection des données et de la vie privée. Chaque région (Union européenne, États-Unis, etc.), administration et entreprise gère actuellement cette protection à sa manière. Face à cet impact géopolitique, les entreprises ont dû revoir leur politique de gestion et de protection de la vie privée des individus et des informations les concernant, mais aussi leur politique d'implémentation des solutions de Big Data basées sur le cloud.

L'adoption du Big Data a également une incidence sur l'exécution des projets informatiques dans les entreprises. La plupart des projets de Big Data sont particulièrement gourmands en technologies et en données. Leurs technologies sont complexes et la main-d'œuvre qualifiée plutôt rare, si bien que les dépassements de délais et de budget sont monnaie courante.

La croissance du Big Data a entraîné une hétérogénéité des entrepôts hébergeant les données personnelles, comme les dossiers médicaux, les coordonnées de cartes bancaires et les données de transaction. Le stockage et l'analyse de ces données ont accentué les pressions que subissent les organisations pour se conformer aux réglementations relatives aux données et à la protection de la vie privée, comme la norme PCI DSS (Payment Card Industry Data Security Standard) et les lois UK Data Protection Act de 1998 et US Health Insurance Portability and Accountability Act (HIPAA). Le respect de ces exigences passe par une démarche pragmatique.

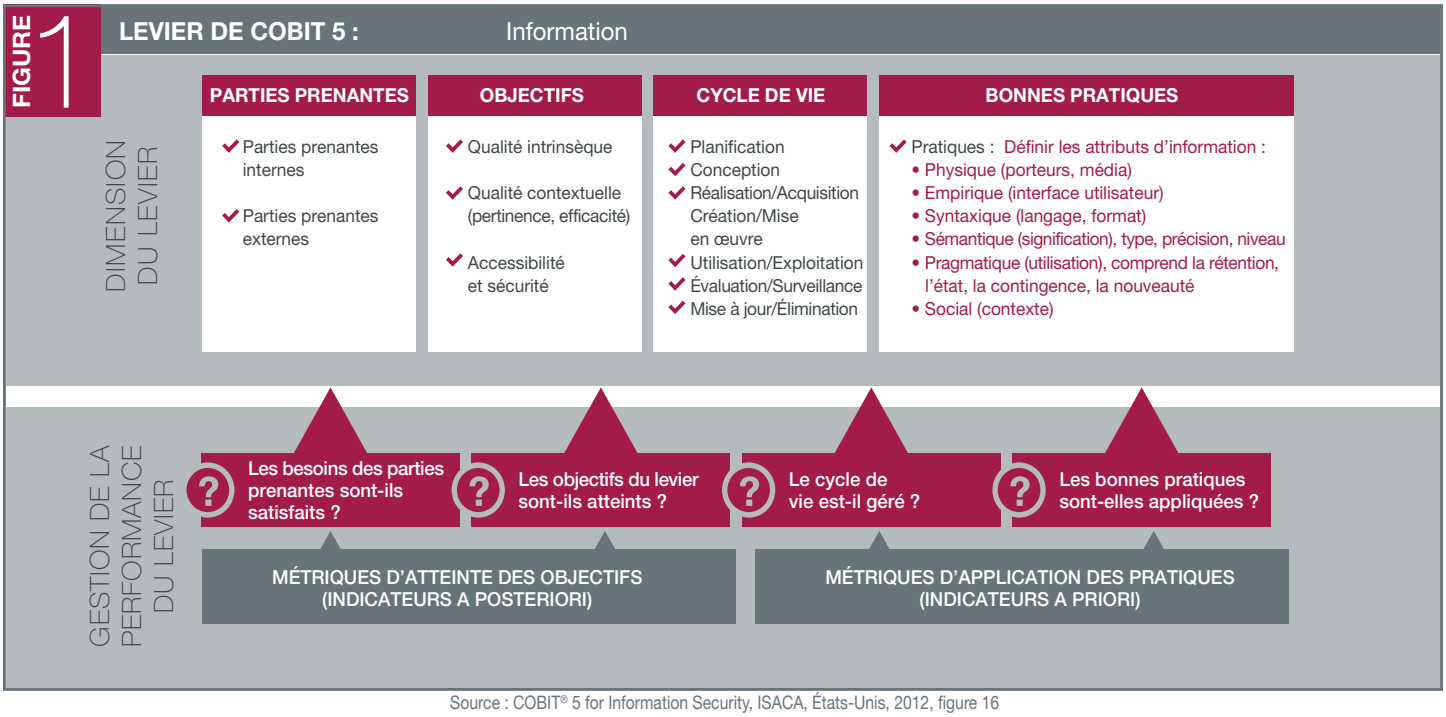
La gestion journalière et en temps réel de données de cette importance est inédite et fait apparaître de nouveaux défis :

- **Complexité de l'évolution technologique**
- **Confidentialité et intégrité des données**
- **Sécurité des données au repos et en mouvement**
- **Disponibilité et résilience des systèmes de données (infrastructure technique)**
- **Traitement des incidents et gestion des failles de sécurité**
- **Gouvernance, gestion des risques et conformité**
- **Gestion des identités et des accès**
- **Pénurie de main-d'œuvre qualifiée**

Le Big Data étant par nature vulnérable aux failles de sécurité et au non respect de la vie privée, il est urgent de trouver un moyen de s'en prémunir. La mise en place de telles mesures se heurte cependant à un certain nombre de difficultés :

- **Complexité sans cesse accrue de l'environnement informatique**
- **Croissance exponentielle des volumes de données transactionnelles**
- **Apparition en masse de nouveaux types de manipulation de données (médias sociaux, appareils)**
- **Utilisation de composants et outils logiciels Java non sécurisés, tels qu'Apache™ Hadoop® et son modèle de programmation MapReduce**
- **Existence de menaces internes et externes**
- **Existence de menaces avancées persistantes (APT)**

Les entreprises et les autorités administratives sont chaque jour confrontées à des violations de données, un phénomène récurrent préoccupant.



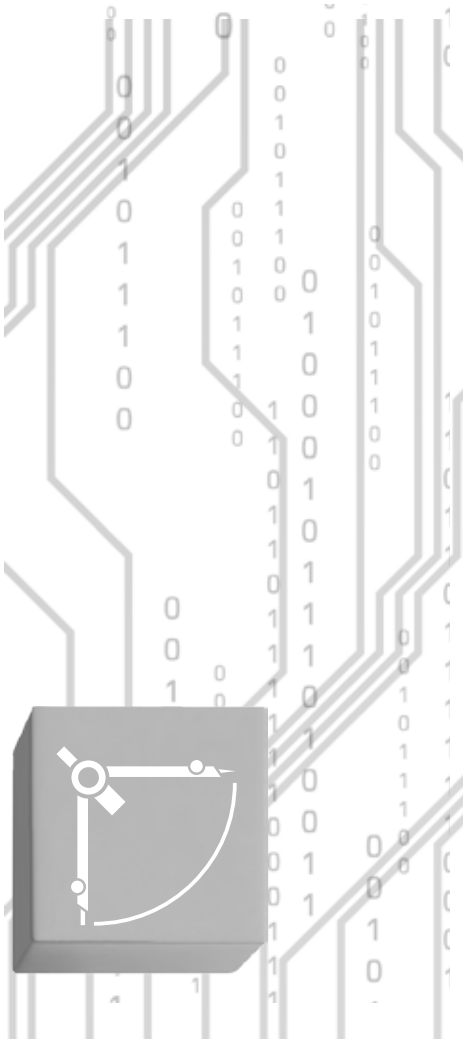
Source : COBIT® 5 for Information Security, ISACA, États-Unis, 2012, figure 16

Outre la publicité négative qu'elles engendrent, ces violations ont des répercussions profondes sur l'entreprise, y compris en termes financiers (amendes pour infraction à la réglementation, frais de contentieux, honoraires de consultants, perte de clients, etc.). Les entreprises sont donc en quête de solutions de protection de la vie privée fiables capables de prévenir les fuites de données et d'assurer la sécurité de ces dernières pendant leur transfert d'un point à un autre, et par-delà les frontières.

Le rythme de croissance des volumes de données de Big Data est tel que ces nouvelles stratégies se doivent d'être évolutives. Les entreprises ont donc besoin de solutions robustes afin de prévenir les vols de données et d'assurer la sécurité de ces dernières dans un environnement informatique complexe. Elles doivent permettre à l'entreprise d'effectuer les tâches suivantes :

- **Identifier toutes les données sensibles**
- **Garantir l'identification et la protection des données sensibles**
- **Assurer la conformité à l'ensemble des lois et réglementations en vigueur**
- **Surveiller de manière proactive les données et l'environnement informatique**
- **Réagir rapidement face à une fuite de données ou à une atteinte à la vie privée grâce à un système de gestion des incidents**

Les phases du cycle de vie du levier information de COBIT 5 (planification, conception, réalisation/acquisition, utilisation/exploitation, surveillance et élimination), représentés **figure 1**, aident les entreprises à gérer ces fonctions et à rationaliser la gouvernance, la gestion des risques et l'exécution sans faille des projets de mise en œuvre de Big Data.



Risques associés à la protection de la vie privée

Utilisée et appliquée à bon escient, l'analyse prédictive du Big Data est un outil formidable. Si la collecte de données en apparence sans lien entre elles ne présente pas de danger en soi, son pouvoir prédictif dépasse, lui, toutes les attentes. Par exemple, le secteur de la santé voit dans le Big Data un moyen de prévoir le comportement des patients et leur état de santé futur. Le service Google Now™, qui suit la position d'un utilisateur via son appareil mobile, ses événements d'agenda, ses requêtes de recherche et ses préférences personnelles, est capable de prévoir ses besoins en informations et d'afficher ces dernières sur son appareil. Grâce aux données personnelles ainsi collectées par Google Now et les transactions de carte de paiement, le secteur de la santé est à même, par l'analyse prédictive, de classer les patients selon leur hygiène de vie. L'analyse prédictive étant toutefois susceptible d'établir un classement erroné d'un individu en présence d'un seul paramètre de suivi, les entreprises doivent recourir à un certain nombre de filtres et de vérifications par recoupement.

Les risques liés au Big Data peuvent être de deux sortes, opérationnels et informatiques, et peuvent être réduits par la mise en œuvre d'une gouvernance solide.

Le risque opérationnel englobe les facteurs externes et internes, notamment le risque géopolitique et la nécessité de satisfaire au plus vite le conseil d'administration et les cadres dirigeants, impatients de devancer la concurrence. Le risque géopolitique, induit par les politiques d'un pays, renvoie à un certain nombre de lois : les lois de l'Union européenne qui restreignent le partage et le traitement transfrontaliers, les lois sur la protection de la vie privée qui régulent le commerce en fonction de groupes d'âges et les lois américaines qui empêchent l'étiquetage et le partage d'informations personnelles, privées et financières potentiellement sources d'usurpation d'identité et de transactions frauduleuses. Les lois propres à un secteur d'activités, comme la loi américaine HIPAA, peuvent s'avérer complexes, et leurs clauses sur le transfert de risque manquer de précision ou ne pas être respectées. « Ce ne sont pas les données elles-mêmes qui créent de la valeur ou posent problème, c'est l'utilisation qui en est faite. »[5]

Le conseil d'administration et les cadres dirigeants d'une entreprise peuvent ainsi, dans un souci de compétitivité, imposer la mise en place d'un Big Data aux responsables informatiques, alors même qu'aucune politique de gestion des risques appropriée n'existe. De même, une mauvaise conception des contrôles en matière de développement des applications peut avoir pour résultat une fuite des données et l'accès non autorisé des développeurs à des données privées.

Des méthodes telles que le développement agile peuvent permettre de contrôler les risques tout en laissant la place à une certaine flexibilité. L'utilisation combinée de ces méthodes et de COBIT 5 peut constituer une bonne stratégie de gouvernance, d'acquisition et de développement.

Le risque informatique désigne le risque métier, plus précisément celui associé à l'utilisation, à la possession, à l'exploitation, à l'influence et à l'adoption des technologies de l'information au sein d'une entreprise[6]. Ce risque existe dès lors que les garde-fous sont franchis. Par exemple, une entreprise peut faire l'acquisition d'outils logiciels non pas nécessairement parce qu'ils répondent aux besoins en analyse décisionnelle de leurs futurs utilisateurs, mais parce que les technologues mettent en avant leur évolutivité. Les informaticiens sont parfois tellement concentrés sur le développement et la livraison qu'ils en oublient les sauvegardes les plus élémentaires en matière de planification de la capacité, et que les ressources et les données ne font l'objet d'aucune surveillance ni de planification adéquate.

Les entreprises doivent mettre l'accent sur la confidentialité des informations relatives aux parties prenantes et veiller à ce que les employés ne les divulguent ni pendant leur fonction dans l'entreprise, ni après leur départ. Le risque de divulgation existe ; il est d'autant plus élevé que l'information est devenue la monnaie du 21ème siècle et que des courtiers en données tirent profit de sa vente (technique couramment appelée DaaS (Data as a Service)).

[5] *Op cit* Forum économique mondial, 2013

[6] ISACA.org, *The Risk IT Framework*, États-Unis, 2009, *www.isaca.org/Knowledge-Center/Research/Documents/RiskIT-FW-18Nov09-Research.pdf*

Stratégies en matière de protection de la vie privée

Différents groupes commencent à se préoccuper de la nécessité d'établir des normes pour le Big Data en matière de protection de la vie privée. Un rapport du Forum économique mondial préconise la mise en place d'une réglementation restreignant l'utilisation à la fois des données personnelles et des technologies. La protection de la vie privée pourrait être intégrée aux technologies de sorte que les utilisateurs puissent garder le contrôle de leurs informations[7]. Le rapport suggère que les futurs systèmes de données soient capables d'associer à toutes les informations collectées un code stipulant les préférences des individus quant à l'utilisation de ces dernières[8]. L'association SIIA (Software and Information Industry Association) met en garde contre une surlégislation du Big Data et de la protection de la vie privée, conseillant aux entreprises d'intégrer cet aspect dans leurs politiques. Selon David LeDuc, directeur principal de la SIIA, l'utilisation du Big Data n'est pas incompatible avec la protection de la vie privée des utilisateurs. Il préconise, par exemple, une anonymisation sans délai des données des consommateurs. Avec l'anonymat, tout élément susceptible de permettre l'identification d'un individu est définitivement exclu des données. La SIIA et d'autres groupes industriels sont d'avis que les législateurs, les associations de défense des consommateurs et toute autre partie prenante devraient plancher ensemble à l'élaboration d'une politique.[9]

L'étude des tendances mondiales en matière de gestion de la protection de la vie privée peut aider les organisations à faire leur choix entre une stratégie défensive et une stratégie offensive. Dans le cas d'une stratégie défensive, les entreprises exploitent les informations tout en protégeant la vie privée des individus par le biais de diverses techniques d'encapsulation et de marquage. L'anonymat, qui n'est en rien un frein à l'étude statistique des tendances ni à l'analyse des données, permet le cas échéant de préserver la vie privée des personnes. La stratégie offensive, quant à elle, mise au contraire sur la divulgation des informations, en rappelant au consommateur que les services proposés sont subordonnés à la communication de certaines données. C'est ce type de stratégie qui est mis en œuvre, par exemple, lorsque des entreprises, en contrepartie d'informations personnelles le concernant, proposent gratuitement au consommateur des bons de réduction, un abonnement à un magazine, des fleurs ou encore des services de messagerie ou d'agenda.

Gouvernance de la protection de la vie privée

Le Big Data permet aux entreprises de consulter, de regrouper et d'analyser des quantités de données en constante augmentation (pages Web, habitudes de navigation, signaux de capteurs, emplacement géographique de smartphones, informations génomiques, etc.). S'il constitue une occasion formidable de faire de l'information le principal moteur de création de la valeur, il peut aussi être source de risques non négligeables pour l'entreprise si cette dernière ne l'encadre pas de politiques et de principes exhaustifs. À ce titre, un référentiel de gouvernance est nécessaire pour se faire des pratiques d'utilisation du Big Data un allié sûr.

Sans une gouvernance appropriée, les données sur lesquelles l'entreprise se base pour créer de la valeur ajoutée peuvent conduire à produire des résultats intrusifs et dommageables ainsi qu'à prendre des décisions dévastatrices.

En assurant un équilibre entre la réalisation de profits d'un côté, et l'optimisation des niveaux de risques et des ressources de l'autre, COBIT 5 permet aux entreprises de tirer la meilleure valeur possible des technologies de l'information.

[7] *Op cit* Forum économique mondial, 2013

[8] Lohr, Steve, « Big Data Is Opening Doors, but Maybe Too Many », *The New York Times*, 23 mars 2013, *www.nytimes.com/2013/03/24/technology/big-data-and-a-renewed-debate-over-privacy.html?_r=1&*

[9] Software & Industry Information Association, « Data-Driven Innovation A Guide for Policymakers: Understanding and Enabling the Economic and Social Value of Data », mai 2013, *www.siia.net*

Le but premier des entreprises est de créer de la valeur pour leurs parties prenantes tout en optimisant la gestion des risques et des ressources. Cet objectif ne saurait être atteint sans une bonne gouvernance et un management approprié de l'information et des actifs informatiques. En tant qu'actif d'entreprise, le Big Data entre naturellement dans le cadre du premier principe de COBIT 5 : répondre aux besoins des parties prenantes.

COBIT 5 fait une nette distinction entre gouvernance et management, la responsabilité de la gouvernance incombant au conseil d'administration de l'entreprise. Les besoins des parties prenantes relatifs au Big Data sont pris en compte et gérés au plus haut niveau de l'entreprise. Dans le tableau RACI de COBIT 5, illustré à la **figure 2**, qui reprend l'un des processus de gouvernance d'entreprise, on voit que le conseil d'administration approuve les initiatives critiques, tandis que la responsabilité du management revient au directeur général et au directeur des systèmes d'information. Ce tableau attribue les niveaux de responsabilités concernant les activités d'un processus à des acteurs et des structures. Les acteurs de l'entreprise apparaissent sur fond rouge, ceux de l'informatique sur fond bleu. Les différents niveaux d'implication sont les suivants :

R (Responsible)—(Responsable) Gère l'enjeu opérationnel principal en réalisant la tâche indiquée et en garantissant le résultat escompté

A (Accountable)—(Approuve ou a autorité) A l'autorité pour mener à bien la tâche

C (Consulted)—(Consulté) Fournit des informations

I (Informed)—(Informé) Reçoit des informations sur la réalisation et/ou les livrables de la tâche

FIGURE 2

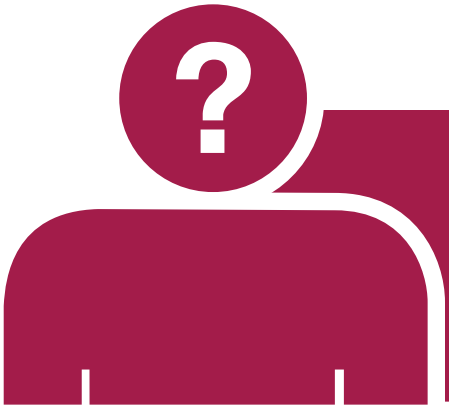
COBIT 5 EDS01 :

Affectation des rôles pour le processus Assurer la mise en place et la mise à jour du référentiel de gouvernance

EDS01 Tableau RACI

Source : COBIT® 5 : Enabling Processes, ISACA, États-Unis, 2012, page 31

EDS01.03 Surveiller le système de gouvernance	EDS01.02 Diriger le système de gouvernance	EDS01.01 Évaluer le système de gouvernance	PRATIQUE DE GOUVERNANCE PRINCIPALE
A	A	A	Conseil d'administration
R	R	R	Directeur général
C	C	C	Directeur financier
C	C	C	Directeur des opérations
R	R	R	Responsables métier
I	I		Propriétaires des processus métier
R	R	R	Comité exécutif sur la stratégie
I	I		Comité de direction (programmes ou projets)
I	I		Bureau de gestion des projets
I	I		Bureau de gestion de la valeur
C	C	C	Directeur des risques
I	I		Directeur de la sécurité de l'information
I	I	C	Comité d'architecture
I	I	C	Comité des risques d'entreprise
I	I	C	Directeur des ressources humaines
C	C	C	Conformité
C	C	C	Audit
R	R	R	Directeur des systèmes d'information
C	C	C	Responsable de l'architecture
I	I	C	Responsable des développements
I	I	C	Responsable des opérations
I	I		Responsable administratif
I	I		Chef de service
I	I		Responsable de la sécurité de l'information
I	I		Responsable de la continuité d'activité
I	I		Responsable de la protection de la vie privée



Pour définir une gouvernance appropriée en matière de protection de la vie privée, le conseil d'administration et les cadres dirigeants doivent se poser les questions suivantes :

Le conseil d'administration et les cadres dirigeants doivent intégrer la dimension informatique dans leurs décisions afin d'élaborer les politiques, processus et procédures appropriés et d'affecter le personnel compétent correspondant.

En entreprise, protéger la vie privée consiste à respecter les lois et les réglementations relatives à la conservation des données, les lois transfrontalières ainsi que les lois sur la protection de la vie privée et la propriété intellectuelle (PI). La gouvernance est là pour veiller à ce respect, mais pas seulement. Elle est aussi gage de compétitivité durable pour l'entreprise qui utilise à bon escient le Big Data.

- Quels principes, politiques et infrastructures mettre en place pour gérer la stratégie de l'entreprise liée au Big Data ?
- Nos sources de Big Data sont-elles fiables ?
- De quelles structures et compétences disposons-nous pour assurer la gouvernance et le management des technologies de l'information ?
- De quelles structures et compétences disposons-nous pour assurer la gouvernance en matière de protection de la vie privée ?
- Disposons-nous des outils appropriés pour satisfaire aux exigences de protection de la vie privée ?
- Comment vérifier l'authenticité des données ?
- Disposons-nous d'un moyen de contrôle sur l'utilisation des informations ?
- Quelles sont nos options en matière de protection de la vie privée ?
- Dans quel contexte les décisions sont-elles prises ?
- Est-il possible de simuler les décisions afin d'en appréhender les conséquences ?
- Est-il prévu de consigner et d'exploiter ces conséquences afin d'optimiser les processus de collecte, d'analyse et de prise de décision ?
- Comment protéger nos sources, nos processus et nos décisions du vol et de la corruption ?
- Exploitons-nous les connaissances tirées du Big Data ?
- Quelles informations peuvent être collectées sans exposer l'entreprise à des contentieux juridiques ?
- Quelles actions prenons-nous susceptibles de créer des tendances exploitables par nos concurrents ?
- Quelles politiques appliquons-nous pour être sûr que les employés ne divulguent pas les informations sur nos parties prenantes pendant leur fonction dans l'entreprise et après leur départ ?

Considérations relatives à l'assurance

Les principaux moteurs concernant l'assurance sont les suivants :

- **Fournir aux parties intéressées une opinion étayée sur la gouvernance et le management des SI en fonction des objectifs d'assurance**
- **Définir des objectifs d'assurance en adéquation avec les objectifs de l'entreprise, de sorte à donner plus de valeur aux initiatives en la matière**
- **Répondre aux exigences réglementaires ou contractuelles afin d'apporter l'assurance nécessaire quant aux dispositions informatiques**

L'avis des professionnels de l'assurance doit être pris en compte dès le départ dans toute initiative de l'entreprise relative au Big Data. Pour pouvoir aider utilement l'entreprise, ces professionnels doivent posséder une solide connaissance de cette dernière, les connaissances qui leur permettent, en tant qu'expert en science des données, d'utiliser les outils du Big Data (Hadoop, la plateforme EMC® Greenplum®, les applications analytiques et les logiciels de base de données Teradata®, le système d'analyse HP™ Vertica™, les logiciels Palantir Technologies, etc.) ainsi que les compétences nécessaires pour interpréter les résultats et les présenter clairement aux parties prenantes. Ils doivent se tenir informés des nouvelles exigences en matière de Big Data, et former la direction et l'équipe d'audit en conséquence.

En plus de renseigner la direction sur le Big Data, les professionnels de l'assurance doivent s'assurer des points suivants :

- **la mise en place de solutions de sécurité et de protection de la vie privée,**
- **l'existence d'une gouvernance suffisante en matière de protection de la vie privée pour le Big data, notamment :**
  - anonymisation des données/suppression de toute information susceptible de permettre l'identification des personnes,
  - mise en place de politiques , processus et procédures appropriés, pertinents, utiles et actualisés ainsi que de structures afférentes,
  - adhésion des cadres dirigeants et assurance de leur engagement dans le temps,
  - mise en place d'une politique clairement définie en matière de management et de destruction des données, et attribution des responsabilités,
  - conformité aux exigences juridiques et réglementaires,
  - formation et sensibilisation continues aux politiques, processus et procédures relatifs au Big Data.

Conclusion

Face à un Big Data de plus en plus omniprésent, il est impératif pour les entreprises de mettre en place les moyens qui leur permettront d'en tirer le meilleur parti. Le champ d'études du Big Data étant centré sur l'individu, une attention toute particulière doit être accordée à la protection de la vie privée. À défaut, les répercussions pourraient être graves.

Si le Big Data est un actif précieux, il constitue aussi un outil puissant à l'impact considérable. C'est la raison pour laquelle le conseil d'administration et les cadres dirigeants doivent conserver une entière visibilité sur ce dernier.

Le succès des entreprises dépend entièrement de la manière dont elles gèreront les différents défis liés au Big Data et ses impacts, notamment sur la vie privée. **Pour tirer le meilleur parti du Big Data et disposer de solutions d'analyse rapides et résilientes, les entreprises doivent recourir à des processus et des référentiels reproductibles parallèlement à une gouvernance et à une gestion des risques appropriées.**