الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Ecole Nationale Supérieure de Management
Koléa

وزارة التعليم العالي و البحث العلمي

المدرسة الوطنية العليا للمناجمنت
القليعة

MÉMOIRE DE FIN D'ÉTUDES

En vue de l'obtention d'un Master académique en Management « GOUVERNEMENT ELECTRONIQUE »

L'impact de la gouvernance électronique Sur la sécurité des données. Cas : Direction générale d'Algérie Télécom

Elaboré par :

BENKHATTOU Rania Ibtissem

LEKHCHINE Ibtihel

Encadré par :

Dr. Mehdi BOUCHETARA

Pr. Messaoud ZEROUTI

Année universitaire 2023-2024

RESUMÉ

Notre étude a pour objectif d’examiner l'impact de la gouvernance électronique sur la sécurité des données. Elle apporte à la littérature de nouveaux résultats empiriques. Nous avons effectué une enquête auprès de 120 employés d'Algérie Télécom à l'aide d'un questionnaire. Nous avons utilisé la méthode quantitative à travers IBM SPSS Statistiques 25 permettant de tester les hypothèses de la recherche. L’analyse est effectuée avec une régression linéaire. Les résultats indiquent un niveau de satisfaction modéré concernant l'implication de la gouvernance électronique dans la sécurité des données. L'analyse de cette recherche empirique révèle qu'améliorer la sensibilisation et la formation (53 % pour chacune) en matière de gouvernance électronique et de sécurité des données a un impact positif sur la culture de sécurité organisationnelle. Cette amélioration de la conscience et des connaissances conduit à une réduction des risques liés aux données, favorisant ainsi une confiance accrue chez les clients et les employés quant à la protection de leurs informations personnelles.

Mots-clés : gouvernance électronique, sécurité des données, satisfaction, protection des informations personnelles.

ABSTRACT

Our study aims to examine the impact of e-governance on data security. It contributes new empirical findings to the literature. We conducted a survey with 120 employees of Algeria Telecom using a questionnaire. We employed a quantitative method through IBM SPSS Statistics 25 to test the research hypotheses. The analysis is conducted using linear regression.

The results indicate a moderate level of satisfaction regarding the involvement of e-governance in data security. The analysis of this empirical research reveals that improving awareness and training (53% for each) in e-governance and data security has a positive impact on organizational security culture. This enhancement in awareness and knowledge leads to a reduction in data-related risks, thereby fostering increased trust among clients and employees in the protection of their personal information.

Keywords: e-governance, data security, satisfaction, protection of personal information.

الملخص

تهدف دراستنا الى قياس تأثير الحوكمة الإلكترونية على أمن البيانات. تقدم هذه الدراسة نتائج جديدة للدراسات السابقة من خلال نتائجها التجريبية. لقياس ذلك اجرينا دراسة تجريبية عن طريق استبيان، على عينة من 120 موظف في شركة اتصالات الجزائر. قمنا باستخدام المنهج الكمي من خلال برنامج IBM SPSS STATISTICS 25الذي مكننا من اختبار فرضيات البحث. تم إجراء التحليل باستخدام الانحدار الخطي .تظهر النتائج مستوى متزايد من الرضا بشأن مشاركة الحوكمة الإلكترونية في أمن البيانات. وتظهر التحليلات التي أجريت على هذه الأبحاث أن تحسين الوعي والتدريب المناسب للعمال (53% لكل منهما) في مجال الحوكمة الإلكترونية و سلامة البيانات يؤثر إيجابا على ثقافة امن المؤسسة. يؤدي هذا التحسين في الوعي والخبرة إلى تقليل المخاطر المتعلقة بأمن البيانات، مما يزيد من الثقة لدى العملاء والموظفين في حماية معلوماتهم الشخصية.

الكلمات المفتاحية : الحوكمة الإلكترونية، أمن البيانات، الرضا، حماية المعلومات الشخصية.

REMERCIEMENTS

La rédaction de ce mémoire a été une expérience incroyablement enrichissante pour nous deux, nous permettant d'acquérir de précieuses leçons de patience et de persévérance à travers les défis pratiques et les interactions humaines rencontrés sur le terrain.

Tout d'abord, nous tenons à exprimer notre profonde gratitude envers Dieu.

Nos sincères remerciements s'adressent en premier lieu à notre encadrant, le Dr. BOUCHETERA Mehdi, pour sa bienveillance et son professionnalisme. Nous vous remercions chaleureusement pour la qualité de votre enseignement et vos précieux conseils qui nous ont guidés vers la réussite de notre mémoire. Nous espérons avoir répondu à vos attentes avec la rigueur nécessaire.

Nous exprimons notre gratitude envers nos familles nos amis et nos proches pour leur soutien moral indéfectible, leur patience et leurs encouragements constants tout au long de cette aventure que nous avons menée ensemble.

Nous remercions également nos camarades et notre école, pour nous avoir offert 2 années exceptionnelles.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

AAA : Authentication, Authorization, Accounting.

ANSSI : L'Agence nationale de la sécurité des systèmes d'information.

API: Application programming interface.

CASB: Cloud Access Security Broker.

CCPA : Loi californienne sur la protection de la vie privée des consommateurs.

CENELEC : Comité européen de normalisation électrotechnique.

CIA : Confidentiality, Integrity, Availability.

CNIL : Commission Nationale de l'Informatique et des Libertés.

CNPE : Conseil National des Participations de l'État.

DLP : Data LeakPrevention,

EGDI : L'index de développement de l'e-gouvernement.

ENISA : L'Agence européenne pour la cybersécurité.

EPI : Indice de participation électronique.

HIPAA: Health Insurance Portability and Accountability Act.

IDO : Internet des objets.

L'UE : L'Union européenne.

NSA : National Security Agency.

OCDE : L'Organisation de Coopération et de Développement Économiques.

PIB : Produit intérieur brut.

RGPD : Règlement général de protection des données.

SPSS: Statistical Package for the Social Sciences

TIC : Technologies de l'information et de la communication.

VPN : Réseau Privé Virtuel.

INTRODUCTION

1.1.Contexte de l’étude

La gouvernance électronique désigne l'utilisation des technologies de l'information et de la communication (TIC) par les entités gouvernementales afin d'améliorer l'efficacité et la transparence des services publics qu'ils offrent (Ndou, V. D., 2004).

La progression constante de la numérisation des services gouvernementaux et l'ampleur de la collecte de données personnelles ont élevé la sécurité des données au rang de préoccupation majeure au cours des récentes années (Alenezi, Tarhini, Masa'deh, Alalwan, & Al-Qirim, 2017). La mise en place d'une gouvernance électronique revêt une importance capitale dans l'élaboration de politiques, de normes et de cadres réglementaires visant à garantir la confidentialité, l'intégrité et la disponibilité des données sensibles (Rusu & Gheorghe, 2017).

Des mesures de sécurité robustes, telles que le chiffrement, l'authentification et le contrôle d'accès, sont essentielles pour protéger les données contre les menaces internes et externes (Khan, Shakil, & Alam, 2020).

Cependant, la réussite de la sécurité des données dans la gouvernance électronique repose non seulement sur des technologies performantes, mais également sur des éléments humains et organisationnels. La sensibilisation, la formation et la conformité des employés sont cruciales pour garantir une protection efficace des données (Sá, Rocha, & Cota P., 2016). La transparence et la responsabilité intégrées dans la gouvernance électronique peuvent accroître la confiance des citoyens en ce qui concerne la protection de leurs données personnelles (Lio, Liu, & Ou, 2011).

Un aspect essentiel de la gouvernance électronique consiste à mettre en place des normes et des réglementations visant à garantir la sécurité et la confidentialité des données. L'OCDE a émis des recommandations sur la stratégie de sécurité numérique pour gérer les risques liés aux données, mettant en avant le rôle crucial de la gouvernance dans le domaine de la cybersécurité (OECD, 2014).

De même, l’union européenne a mis en place le Règlement Général sur la Protection des Données (RGPD) qui impose des normes rigoureuses pour la protection des données personnelles, y compris pour les entités gouvernementales. La conformité au RGPD exige une gouvernance solide en matière de sécurité des données (Tikkinen-Piri, Rohunen, & & Markkula, 2018).

De nombreux pays ont instauré des lois et des réglementations nationales pour renforcer la sécurité des données dans le cadre de la gouvernance électronique. Par exemple, en 2014,

les États-Unis ont mis en place la loi sur la modernisation de la cybersécurité pour le gouvernement fédéral (Cárcamo, Bernabe, Navarro, Racero, & Monreal, 2017).

Néanmoins, assurer une sécurité efficace des données dans le cadre de la gouvernance électronique demeure un défi. Selon une étude réalisée par (Al-Rashdi, 2013) les principaux obstacles comprennent un manque de sensibilisation, de ressources et de cadres de gouvernance appropriés.

1.2.Objectifs de l'étude

L'objectif principale de cette étude est d'examiner les mécanismes de gouvernance électronique qui sont mis en place pour garantir la sécurité des données, à identifier les éléments qui peuvent renforcer ou affaiblir cette sécurité, et à formuler des recommandations pour améliorer la protection des données dans un environnement numérique en constante évolution dans le contexte algérien.

Toutefois, des objectifs secondaires et complémentaires peuvent être identifiés, nous citons

- Approfondir les connaissances dans le domaine de la gouvernance électronique et la sécurité des données.
- Analyser les défis et les risques liés à la sécurité des données dans un contexte de gouvernance électronique.
- Avoir connaissance de l'état des lieux de la gouvernance électronique et de la sécurité des données en Algérie.

1.3. Problématique

Dans le but d'identifier l'impact de la gouvernance électronique sur la sécurité des données chez les employés d'Algérie télécom, la présente recherche vise à répondre à la question de recherche qui s'articule sur les travaux des auteurs (Poussing & Dagorn, 2012) (Sylva, Maurel, Bruyère, Saint-Germain, & Gareau, 2019) (Bentounsi, Cante, Coya, Darmon, Chambourcy, & al, 2019) (Ullah, F.; Sepasgozar, S. M.; Wang, C., 2019). Nous nous accordons à établir la problématique qui suit :

Quel est l'impact de la gouvernance électronique sur la sécurité des données ?

1.4. Les hypothèses

Afin de répondre à la question de recherche ci-dessus et À partir d'une analyse de la littérature (Ullah, F.; Sepasgozar, S. M.; Wang, C., 2019) (Aloufi, A. A.; Vasarhelyi, M. A., 2022) (Tomo, A.; Todisco, M.; Ruggieri, M.; Vinci, M. B., 2021) (Zissis, D.; Lekkas, D., 2012) nous avons identifié ces hypothèses :

-H0: Une formation adéquate des employés sur la gouvernance électronique et la sécurité des données, combinée à une transparence dans la gouvernance électronique, pourrait renforcer la culture de sécurité, réduire les risques de violation des données et accroître la confiance des clients et des employés dans la protection de leurs données personnelles.

-H1: Bien que censée renforcer la protection des données, l'implémentation de la gouvernance électronique risque de ne pas réduire substantiellement les menaces contre la sécurité des données.

1.5.Méthode

Pour répondre à notre question de recherche et vérifier nos hypothèses, nous allons réaliser une enquête quantitative. (Venkatesh, Morris, Davis, & Davis, 2003) (Abraham, Schneider, & vom Brocke, 2019) (Bentounsi, Mehdi; Cante, Edouad; Coya, Daniel; Darmon, Patrice; Chambourcy, Arnaud; Gnokam, Gisèle, 2019) en utilisant un questionnaire adressé aux employés de la direction générale d'Algérie télécom.

1.6.L’intérêt de la recherche

Notre étude se concentre principalement sur un problème majeur d’actualité, une gouvernance électronique solide pour protéger les données sensibles des citoyens contre les accès non autorisés, les fuites ou les cybers menaces.

1.7. Plan du document

Le présent document est organisé de la manière suivante :

L'introduction offre un aperçu du contexte et de l'importance de la recherche, des objectifs poursuivis, ainsi que de la problématique et des hypothèses examinées à travers la méthodologie de recherche appliquée.

Le Chapitre I présente l’état de l’art, il comporte deux (3) sections : la section (1) est dédiée à la revue de littérature ; la section (02) se focalise sur le cadre conceptuel de la recherche et la section (03) se concentre sur la gouvernance électronique des données et la sécurité des données.

Le chapitre II se divise en trois parties du cadre méthodologique. La première partie intitulée "Méthode", détaille la méthode de travail et de collecte de données utilisée. La seconde partie, intitulée "Données", expose la population et l'échantillon de notre étude, ainsi que les variables de mesure. La troisième partie, présente Algérie Télécom.

Le chapitre III expose les résultats de l'étude quantitative réalisée. Ces résultats sont ensuite discutés et comparés à ceux issus de la revue de littérature présentée au Chapitre I.

En dernier lieu, la conclusion récapitule les résultats clés obtenus dans le cadre de notre étude. Elle met également en lumière les limites de la recherche et propose des suggestions pour de futures investigations, ouvrant ainsi la voie à un approfondissement du sujet.

CHAPITRE I : CADRE THÉORIQUE

Section 1 : Revue de littérature

Dans cette section, nous présentons la revue de littérature constituée de plusieurs études effectuées sur « l'impact de la gouvernance électronique des données sur la sécurité des données », après une recherche approfondie nous avons pu assembler plusieurs études qui se rapproche de notre sujet, l'objectif est de positionner l'étude dans les champs de recherche de la gouvernance.

1. Positionnement de la recherche dans le champ de la gouvernance

Au 20^{e} siècle, l'essor de l'informatique et des technologies de communication a révolutionné, la façon dont les données sont collectées, stockées, et analysées. Les bases de données informatiques ont permis une manipulation plus rapide et efficace des données à grande échelle. Aujourd'hui, nous vivons « l'ère de la donnée massive », ou d'énormes quantités de données sont générées chaque jour grâce aux appareils connectés.

L'augmentation rapide des données générées par les humains et les machines a fait prendre conscience aux entreprises du potentiel stratégique des données. Avec ce rôle changeant des données, les entreprises doivent mettre en œuvre efficacement un ensemble de mécanismes de gouvernance pour atteindre leurs objectifs stratégiques et améliorer les performances organisationnelles. La gouvernance des données fait référence à l'exercice de l'autorité et du contrôle sur la gestion des données. Le but de la gouvernance des données est d'augmenter la valeur des données et de minimiser les coûts et les risques liés aux données. Malgré l'importance croissante de la gouvernance des données ces dernières années, une vision holistique de la gouvernance des données, qui pourrait guider à la fois les praticiens et les chercheurs, fait défaut. (Abraham, Rene; Schneider, Johannes; Brocke, vom, 2019)

2. L'écosystème de la gouvernance des données

Le rôle de la gouvernance des données est double : d'une part, elle vise à gérer les risques en garantissant la sécurité, l'intégrité et la protection des données et des systèmes, et d'autre part, elle cherche à optimiser la valeur des données en établissant des règles et des normes techniques pour faciliter le transfert, la combinaison et l'échange des données de manière plus efficace. Ces niveaux de gouvernance contribuent à instaurer un climat de confiance quant à la manière dont les données sont produites, collectées, traitées et utilisées. La gouvernance des données dépasse la simple gestion des données en établissant des normes et des règles concernant les droits, les principes et les obligations liés à l'utilisation des données. Les principes, stratégies, politiques, lois, règlements et normes de gouvernance

des données sont élaborés par les institutions et les acteurs de l'écosystème des données. Cet écosystème englobe non seulement les gouvernements, mais également des acteurs non gouvernementaux tels que les organisations de la société civile, le secteur privé, les universitaires, et d'autres parties prenantes qui ont un intérêt et un rôle à jouer dans la manière dont les données doivent être gouvernées. (Banque Mondiale, 2021)

En tenant compte des contributions des auteurs (Da Sylva, Maurel, Bruyère, Saint-Germain, & Gareau, 2019) la gouvernance des données exerce des impacts observables sur tous les aspects de l'écosystème. Elle influence en partie les éléments d'information intégrés à cet écosystème, suite à des décisions prises par des acteurs-clés. Elle joue un rôle crucial dans les dynamiques de pouvoir et de collaboration entre les parties prenantes, régissant les processus définis et les opérations appliquées aux objets d'information. De plus, le cadre juridique et réglementaire est étroitement lié aux intervenants, aux objets d'information et aux processus en place. Ainsi, il est évident que l'écosystème décrit par ce projet constituera un modèle d'étude de la gouvernance des données.

3. L’engagement des organisations dans la gouvernance de la sécurité de l'information

Dans une étude intitulé « Engagement et pratiques des organisations en matière de gouvernance de la sécurité de l’information » (Poussing, Nicolas; Dagorn, Nathalie, 2012) les chercheurs ont conclu que la connaissance d'autres organisations engagées dans la gouvernance de la sécurité de l'information, la performance espérée et l'effort déployé sont des déterminants de l'engagement des organisations dans cette démarche.

Ces résultats visent à examiner le processus d'engagement des organisations dans la gouvernance de la sécurité de l'information ainsi que les pratiques de gouvernance de la sécurité de l'information au sein des organisations engagées dans cette démarche.

Les deux chercheurs ont opté pour une enquête conduite auprès de cent vingt grandes entreprises luxembourgeoises. Les données ont été analysées à l'aide de techniques statistiques et économétriques.

L’étude a montré que l’originalité majeure de cette recherche réside dans le taux de participation très important (85,71%) à l’enquête qui a été menée. Elle permet d'établir un état des pratiques actuelles de gouvernance de la sécurité de l'information mises en œuvre par les organisations engagées dans la démarche.

En résumé, l’article met en lumière les facteurs qui influencent l’engagement des organisations dans la gouvernance de la sécurité de l’information et fournit un aperçu des

pratiques actuelles en la matière. Ses résultats peuvent être utiles aux managers, aux chercheurs et aux décideurs publics intéressés par la sécurité de l'information dans les entreprises.

4. La gouvernance des données comme accélérateur de conformité au règlement général sur la protection des données

Dans une étude menée par (Bentounsi, Mehdi; Cante, Edouad; Coya, Daniel; Darmon, Patrice; Chambourcy, Arnaud; Gnokam, Gisèle, 2019), trouvent que la gouvernance et la protection des données étaient considérées comme des objectifs distincts. Cependant, avec l'entrée en vigueur du RGPD et la demande croissante des individus, les organisations sont désormais tenues de répondre à des exigences renforcées en matière de protection de la vie privée tout en assurant la transparence quant à la collecte, la conservation, l'agrégation, l'utilisation et le partage des données. Pour atteindre ces objectifs, les organisations doivent mettre en place des solutions permettant une meilleure protection des données et fournir des rapports détaillés sur leur utilisation.

Ils présentent ARIANE, une plateforme intégrée de gouvernance des données à caractère personnel et soulignent l'importance de la gouvernance des données pour assurer cette conformité, en insistant sur la nécessité d'intégrer la protection de la vie privée dès la conception des processus métiers et des systèmes d'information.

L'objectif de cette étude est de présenter ARIANE comme un outil permettant d'accélérer de cette conformité des organisations au RGPD.

5. La gouvernance des données et la sécurité dans le secteur bancaire

A l'égard de tous les secteurs, les banques sont tenues de recueillir et de conserver un volume important de données relatives à leurs clients, comprenant des informations confidentielles considérées comme sensibles par la CNIL. Il est donc essentiel pour le secteur bancaire de traiter ces données de manière éthique et de garantir leur sécurité. La digitalisation des opérations bancaires a certes simplifié l'expérience des clients et des collaborateurs, mais elle expose également ces entreprises à de nouveaux risques en raison de la multiplication des cybers attaques.

Donc la protection des données des clients, la sécurisation des transactions et la conformité aux réglementations de confidentialité sont des préoccupations essentielles pour les banques. (Elana, 2023)

Dans une étude intitulée « litiges liés à la vie privée et la sécurité des données dans le secteur bancaire : implication pour la gouvernance d'entreprise », menée par les chercheurs (Hashim, Muhammad; Mahfooz, Bakhtawar; Ibrahim, Kainat, 2023).

L'objectif de l'étude est d'examiner les faiblesses de la gouvernance d'entreprise mise en évidence dans le traitement de ces affaires par les banques et analyser les principaux litiges en matière de confidentialité de sécurité des données, auxquels les banques américaines ont été confrontées au cours de la dernière décennie.

Les chercheurs ont étudié la gouvernance de la banque en matière de sécurité et de protection des données, l'étude a examiné 15 cas de litiges, ils ont utilisé une approche mixte, à travers une analyse de cas et une analyse de régression des paramètres de gouvernance des banques. (Hashim, Muhammad; Mahfooz, Bakhtawar; Ibrahim, Kainat, 2023)

Sur le même axe, une étude assez intéressante réalisée par (Franco, Jean-Michel, 2018), sur la gouvernance des données dans les banques, a démontré que répondre à l'exigence de conformité dans un environnement réglementaire complexe nécessite une gestion de données de haute qualité. La cartographie et l'audit des flux de données, également connus sous le nom de lignage des données, sont des éléments essentiels pour identifier l'origine des données et fournir des preuves de ces analyses aux organismes de contrôle externes.

Il a souligné que pour assurer la conformité, les organisations doivent avoir une compréhension du cycle de vie de leurs données. Elles doivent être en mesure de démontrer, selon les besoins, les processus et les transformations par lesquels ces données évoluent au fil du temps. (Franco, Jean-Michel, 2018).

6. Les blockchains et la protection des données

D'après (Koscina, 2021), qui a exploité l'étude de « sécurité et optimisation des blockchains et des algorithmes associés ». L'auteur a mis en lumière les mécanismes pour protéger le code source du logiciel afin d'éviter l'exploitation des vulnérabilités et pour protéger la propriété intellectuelle, pour objectif de minimiser les problèmes de sécurité auxquels fait face la mise en œuvre de la blockchain, pour assurer la confidentialité des utilisateurs, la gouvernance des données et le développement des modèles de crypto-monnaies pour les économies circulaires.

Les résultats obtenus affirment en premier lieu, l'existence de deux types de solutions : un nouveau protocole de consensus qui préserve la confidentialité des utilisateurs et un nouveau schéma de vote électronique confidentiel utilisant une blockchain permission et

un protocole d’offuscation de graphiques de flux de contrôle pour la confidentialité des logiciels.

En second lieu, les deux résultats de recherche appliqués avec deux prototypes de systèmes blockchain, répondent aux problématiques posées par la gouvernance des données et les crypto-monnaies.

Ce travail vise à créer un algorithme capable de convertir un programme en un nouveau programme équivalent, en se basant sur le graphe de flux de contrôle. L'algorithme utilise des instructions standard (comme les opérations de registre et de pile) et une variable de routage aléatoire pour générer un nouveau graphe de flux de contrôle. (Koscina, 2021)

Dans le même contexte, (Makhdoom, Imran; Zhou, Ian; Abolhasan, Mehran; Lipman, Justin; Ni, Wei, 2020) **dans** leurs travaux, proposent un cadre novateur appelé "PrivySharing" basé sur la blockchain pour le partage sécurisé et respectueux de la vie privée des données IDO dans les villes intelligentes.

Ce cadre se distingue des approches existantes en divisant le réseau blockchain en canaux distincts, chacun traitant un type spécifique de données et limitant l'accès aux organisations autorisées via des règles de contrôle d'accès intégrées dans les contrats intelligents.

Ils ont également présenté un système de récompense sous forme de jeton numérique appelé "PrivyCoin" pour les utilisateurs ayant partagé leurs données avec les parties prenantes/tiers.

Enfin, les résultats expérimentaux ont montré qu'une blockchain multicanaux était plus évolutive qu'un système blockchain monocanal. (Makhdoom, Imran; Zhou, Ian; Abolhasan, Mehran; Lipman, Justin; Ni, Wei, 2020)

7. La gouvernance électronique comme garante de la sécurité des dans le cloud computing

L'article de (Zissis, D.; Lekkas, D., 2012) met en lumière les défis majeurs de sécurité liés à l'adoption du cloud computing et souligne le rôle crucial de la gouvernance électronique pour assurer la protection des données.

Les auteurs identifient plusieurs problématiques clés de sécurité dans le cloud : la sécurité et confidentialité des données, le respect de la conformité réglementaire, les lacunes en matière de gouvernance et d'audit, ainsi que les risques liés à l'isolation et la virtualisation.

Face à ces enjeux, les auteurs préconisent l'adoption de pratiques rigoureuses de gouvernance électronique pour encadrer l'utilisation des services cloud. Ils proposent notamment :

-Le chiffrement robuste des données avant leur stockage dans le nuage afin de garantir leur confidentialité et intégrité.

-La mise en place de contrôles d'accès stricts et d'authentification multi facteur pour restreindre l'accès aux données sensibles.

-Une sélection minutieuse des fournisseurs cloud réputés et conformes en termes de sécurité, transparence et respect des réglementations.

-La conception d'une architecture cloud sécurisée intégrant des contrôles de sécurité à tous les niveaux (infrastructure, applications, données).

8. L'efficacité de la gouvernance électronique et la sécurité des données dépendent de la sensibilisation et de la confiance des citoyens

Dans leur étude, (Ullah, F.; Sepasgozar, S. M.; Wang, C., 2019) ont examiné les défis et opportunités liés à la mise en œuvre de la gouvernance électronique au Bangladesh, mettant en lumière les enjeux de sensibilisation et de confiance citoyenne. Bien que le pays ait instauré des initiatives d'e-gouvernance visant à offrir des services publics en ligne et accroître la transparence gouvernementale, les auteurs soulignent que les préoccupations relatives à la sécurité et la confidentialité des données demeurent prépondérantes au sein de la population.

Les citoyens expriment des craintes quant aux risques d'utilisation abusive ou de divulgation non autorisée de leurs informations personnelles. Ce scepticisme est exacerbé par un manque généralisé de compétences en matière de sécurité informatique, accentuant la vulnérabilité aux fuites de données et cyberattaques. De plus, la faible confiance envers les services gouvernementaux en ligne, alimentée par la perception de corruption et le déficit de transparence, engendre une méfiance à l'égard de l'e-gouvernance.

Néanmoins, l'étude met en exergue certaines opportunités. La sensibilisation des citoyens aux bénéfices de l'e-gouvernance et le renforcement de leur confiance sont identifiés comme des facteurs indispensables à une adoption réussie. La mise en place de mesures de sécurité robustes, de cadres réglementaires solides et d'une meilleure transparence sont susceptibles d'accroître la confiance citoyenne dans la protection des données personnelles.

9. L’impact de la confiance envers le gouvernement électronique sur la participation des citoyens

(Aloufi, A. A.; Vasarhelyi, M. A., 2022) examinent l'influence des éléments de confiance envers l'e-gouvernement sur la participation électronique des citoyens en Arabie saoudite met en évidence l'importance fondamentale de la protection des données et de la

confidentialité. Cette étude identifie quatre éléments essentiels de confiance : la sécurité/confidentialité, la capacité, l'intégrité et la bienveillance. Parmi ceux-ci, la sécurité/confidentialité, incluant la préservation des données personnelles et la sûreté des transactions en ligne, se révèle être l'élément le plus déterminant quant à l'engagement des citoyens.

Les individus en Arabie saoudite démontrent une propension accrue à utiliser les services en ligne lorsqu'ils ont la perception que leurs données sont sécurisées et que leur vie privée est préservée. Toutefois, des appréhensions persistent en ce qui concerne la sécurité des données personnelles et la confidentialité lors de l'usage des services d'e-gouvernement. Ce scepticisme quant à la sécurité des données entrave l'adoption et l'utilisation des services en ligne par les citoyens.

Afin de promouvoir la participation électronique, les auteurs préconisent aux organismes gouvernementaux d'investir dans des dispositifs de sécurité robustes, tels que le cryptage des données et l'authentification renforcée. Une communication transparente sur les pratiques de sécurité des données et les politiques de confidentialité peut renforcer la confiance des citoyens.

En définitive, cette étude souligne l'impératif d'investir dans des dispositifs de sécurité solides et de renforcer la transparence pour contrer les préoccupations relatives à la sécurité des données et ainsi accroître la confiance des citoyens envers l'e-gouvernement, favorisant ainsi leur engagement dans les services en ligne.

10. Conformité à la réglementation sur la protection des données personnelles par la gouvernance des données : un impératif pour la gouvernance électronique

Cette recherche propose une analyse exhaustive des principes et des réglementations afférents à la protection des données personnelles, en mettant en relief l'importance de la conformité par le biais de la gouvernance des données. Les réglementations majeures telles que le Règlement général sur la protection des données (RGPD) de l'Union européenne et les législations nationales sur la protection des données sont passées en revue, toutes visant à assurer la sécurité et la confidentialité des données personnelles des individus dans le cadre numérique.

La gouvernance des données est présentée comme un élément clé pour garantir la conformité avec ces réglementations. Elle implique l'instauration de politiques, de processus et de contrôles visant à gérer de manière responsable les données personnelles

tout au long de leur cycle de vie. Dans ce contexte, la gouvernance électronique (e-gouvernance) émerge comme un acteur central dans la gestion des données personnelles collectées et traitées par les organismes gouvernementaux. Une gouvernance des données robuste au sein de ces entités revêt une importance cruciale pour garantir la sécurité des données des citoyens et assurer la conformité réglementaire.

Néanmoins, cette étude souligne les défis inhérents à la sécurité des données, notamment les cybermenaces, les fuites de données et les violations de la vie privée. Les auteurs alertent sur les conséquences néfastes d'une mauvaise gestion des données personnelles, pouvant entraîner des amendes, des poursuites judiciaires et la perte de confiance des citoyens.

Ainsi, pour faire face à ces enjeux, cette étude recommande aux organismes gouvernementaux d'adopter une approche globale de gouvernance des données, incluant des politiques, des processus, des contrôles et des technologies appropriées. La formation du personnel, la sensibilisation des citoyens et la transparence sur les pratiques de protection des données sont également soulignées comme étant essentielles pour garantir une gestion responsable des données des citoyens. (Tomo, A.; Todisco, M.; Ruggieri, M.; Vinci, M. B., 2021)

Section 2 : Cadre conceptuel

Au cours des dernières années, de nombreux pays ont été témoins de changements majeurs dans la façon dont les gens communiquent et travaillent. Ces changements comprennent une augmentation massive de la quantité d'informations produites et partagées, ainsi que la fusion des technologies de stockage et de communication. De plus, les coûts ont considérablement diminué, tandis que l'équipement informatique et les applications logicielles ont connu une croissance exponentielle. Certains auteurs affirment que ces évolutions ont entraîné la disparition des obstacles traditionnels liés au temps et à la distance dans la communication.

Au milieu des années 1990, l'expression "société de l'information" est apparue pour décrire une nouvelle tendance. Dans cette société, la création, la distribution et la manipulation des informations sont devenues les activités économiques et culturelles dominantes. Les technologies de l'information et de la communication (TIC), les industries de services et le capital intellectuel jouent un rôle décisif dans la production économique. En revanche, les secteurs axés sur la production de masse, les industries de transformation et le travail manuel connaissent un déclin relatif. Cette transition vers une société de l'information s'accompagne de l'émergence d'un nouveau monde du travail, caractérisé par l'apparition de nouvelles "économies du savoir" qui emploient des "travailleurs de la connaissance" familiarisés avec les technologies électroniques.

Les changements qui ont donné naissance à la société de l'information ont également affecté tous les secteurs, y compris le secteur commercial. Cette nouvelle ère a suscité un vif intérêt pour le commerce électronique et les affaires en ligne, avec le potentiel de transformer les performances en termes de services et de productivité organisationnelle. Dans le secteur public, la réponse à ces pressions se traduit par la gouvernance électronique, également appelée "e-gouvernance". (Castells, 2010)

1. L’évolution de la gouvernance électronique

1.1. Définition de la gouvernance électronique

Au fil des ans, la discussion sur la combinaison des TIC et de la gouvernance a évolué, tout comme le débat plus large sur la gouvernance électronique. La gouvernance électronique englobe le gouvernement électronique, mais les conceptualisations des deux concepts ne sont pas encore pleinement développées. Le caractère multidisciplinaire de ces domaines n'a pas encore permis l'émergence d'un champ scientifique solide et indépendant. En se basant sur l'expérience passée, il est possible d'envisager les progrès futurs qui pourraient

influencer les politiques actuelles en matière de gouvernance électronique. (Misuraca, G.; Rossel, P., 2011)

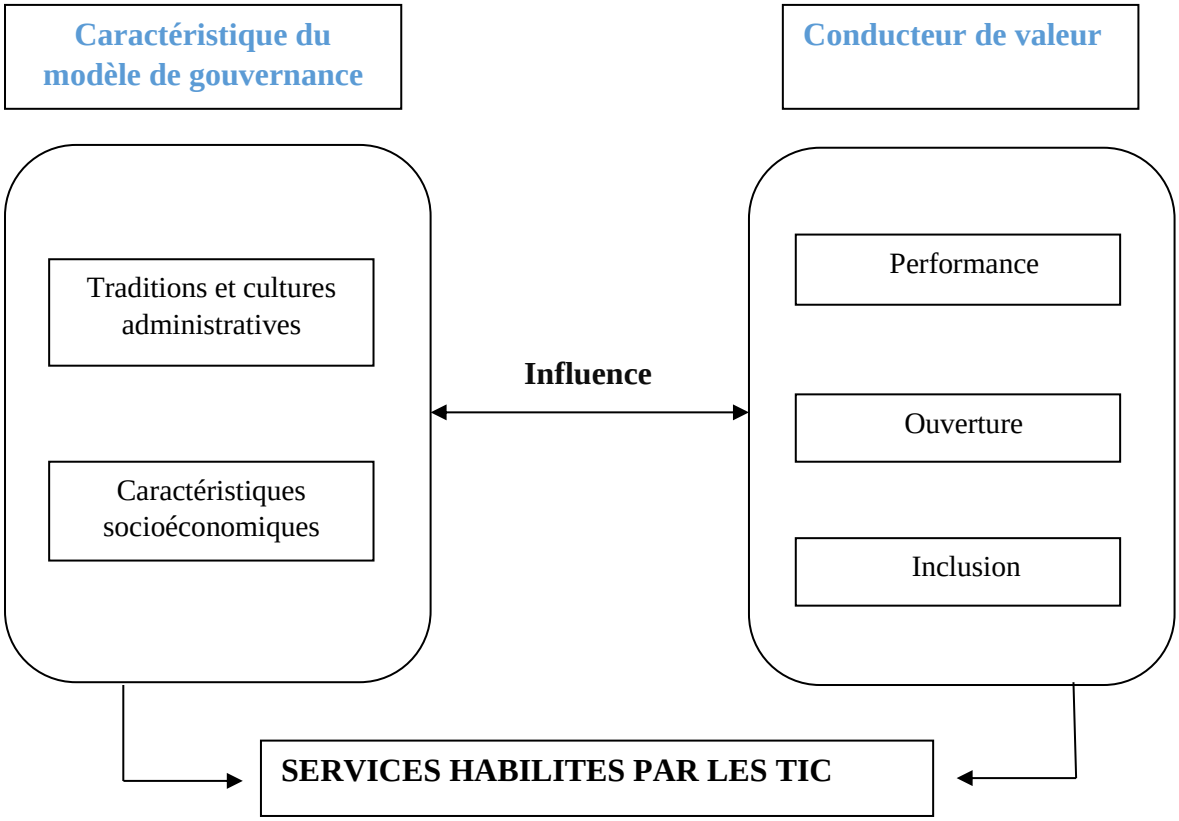
Le cadre théorique sous-tendant la gouvernance électronique est en constante évolution. Comme l'ont montré des travaux antérieurs (Misuraca, G.; Rossel, P., 2007), il est impératif d'envisager un changement de paradigme radical pour conceptualiser cette forme de gouvernance.

Le concept de gouvernance a été examiné selon de multiples perspectives et dans diverses disciplines, ce qui a conduit à des définitions en évolution et à une variété d'interprétations. En science politique et en sociologie, la gouvernance peut être décrite comme un processus de transformation et de reformulation de l'approche des affaires publiques, impliquant la mise en place de systèmes pour coordonner les différents acteurs locaux au sein des sociétés (Jacquier, C., 2008).

Cette vision est en ligne avec une autre définition élaborée par les Nations Unies, qui considèrent la gouvernance comme un ensemble varié d'institutions, de systèmes, de structures, de processus, de procédures, de pratiques, de relations et de comportements de leadership dans l'exercice de l'autorité politique, économique et administrative dans la gestion des affaires publiques ou privées (Unies, Nations, 2003). La gouvernance n'est donc pas simplement une question de gouvernement. C'est un ensemble complexe d'interrelations dans lequel divers acteurs des secteurs public et privé, ainsi que de la société civile, jouent différents rôles – parfois en conflit, parfois en complémentarité – dans le but de servir les intérêts de la communauté locale.

La gouvernance électronique peut être vue comme un cadre global pour observer la coévolution des différents acteurs du domaine des TIC dans leurs relations avec les institutions politiques locales, nationales ou internationales. En même temps, elle devrait être considérée comme un concept multidimensionnel englobant la recherche dans le domaine des TIC, se situant à la frontière de la recherche en sciences sociales, économiques, politiques et organisationnelles, et soutenant la définition des missions gouvernementales en lien avec les intérêts de la société (Misuraca, G., 2009). Ainsi, pour enrichir le débat scientifique et aligner les perspectives de la recherche et des politiques. Cela implique l'utilisation des TIC pour simplifier les opérations administratives, faciliter l'interaction entre gouvernements, citoyens et autres parties prenantes, et promouvoir la participation citoyenne tout en garantissant l'inclusion et l'égalité des chances pour tous. (Misuraca, G., 2010).

Figure 1 : Cadre théorique pour l'interprétation de la gouvernance électronique.



Source : adapté de (Misuraca, Gianluca; Viscusi, Gianluigi, 2010)

1.2. Naissance et émergence de la gouvernance électronique

L'analyse de l'évolution des programmes de gouvernement électronique en Europe au cours de la dernière décennie montre un changement significatif dans les priorités. En 2001, le gouvernement électronique était associé à la modernisation, la réorganisation, l'accès et la participation. En 2003, la transparence, l'efficacité et les mesures sont devenues des thèmes importants. En 2005, à Manchester, l'accent a été mis sur la transformation, l'efficacité, l'inclusion, l'identité et le partage des bonnes pratiques. Le plan d'action i2010 de la Commission européenne, adopté à Lisbonne en 2007, a introduit les mots-clés innovation et interopérabilité. Enfin, à Malmö en 2009, l'agenda politique s'est recentré sur l'engagement, l'ouverture, la qualité des services et les besoins des usagers. (Broster, D.; Misuraca, G.; Bacigalupo, M., 2011).

Au début des années 2000, l'objectif initial consistait à développer une plateforme numérique pour les gouvernements afin de donner aux citoyens un accès diversifié aux services publics. Les technologies de l'information et de la communication (TIC) étaient vues comme un ensemble d'outils destinés à moderniser le secteur public et à améliorer la

prestation de services, favorisant ainsi l'inclusion et une plus grande participation. Au fil du temps, les objectifs ont évolué pour inclure la réduction de la charge administrative, permettant ainsi de libérer des ressources et d'optimiser le rendement de l'investissement des contribuables. Cette approche vise également à stimuler la productivité en augmentant l'efficacité grâce à une utilisation plus efficace des ressources. Pendant cette période, l'importance de l'utilisation transfrontalière de solutions émergentes a considérablement évolué, passant de simples échanges de bonnes pratiques à une coopération plus étroite, des actions concertées et un partage accru des connaissances. Cela a permis le déploiement de systèmes transfrontaliers d'identification électronique et d'authentification. L'interopérabilité est devenue le point central des services intégrés des gouvernements électroniques transfrontaliers, visant à faciliter la mobilité des citoyens et le commerce en éliminant les obstacles procéduraux entravant le marché unique. (Misuraca, G.; M., Rossel P. et Finger, 2006).

En parallèle avec l'évolution du gouvernement électronique, la gouvernance électronique est initialement conçue comme une composante de la réforme de l'administration publique, mais elle devient rapidement un défi social majeur et un mécanisme capable d'améliorer non seulement les services administratifs et la satisfaction des utilisateurs, mais aussi de promouvoir des formes approfondies de démocratie. Alors que le gouvernement électronique démontre l'efficacité de l'administration, la gouvernance électronique a un impact bien plus large en permettant la participation pleine et active de la société civile et du secteur privé. En favorisant les interactions entre les acteurs, cet outil entraîne des changements dans les processus de conception des politiques et des réglementations. (Misuraca, G.; M., Rossel P. et Finger, 2006).

Il est intéressant de noter que, tandis que le débat sur le gouvernement électronique était principalement centré sur les pays industrialisés, la gouvernance électronique a émergé à partir d'expériences sur le terrain dans les pays en développement. (Misuraca, G., 2007).

Un certain engouement pour la gouvernance électronique s'est répandu par la suite dans les pays en développement et émergents, en particulier en Asie du Sud-Est et en Inde. Par exemple, (Basu, S., 2004) examine les questions de lois et d'infrastructures liées à la gouvernance électronique dans ces pays, en mettant l'accent sur leur succès dans l'élaboration de cadres juridiques pour le gouvernement électronique. Cependant, la confusion entre gouvernement électronique et gouvernance électronique, comme dans de nombreux autres cas, n'a pas été dissipée.

Les pays en développement qui ont adopté les technologies de l'information et de la communication (TIC) n'ont pas connu la forte croissance prédite par de nombreux universitaires. Malgré de nombreux projets pilotes et expériences coûteux, les résultats ont souvent été mitigés (Heeks, R., 2001). La promotion de la gouvernance électronique dans ces régions a également été controversée (Chavan, G. R.; Rathod, M. L., 2009). Par exemple, en Inde et en Asie du Sud-Est, il y a eu un intérêt croissant pour la gouvernance électronique et les TIC, mais ces initiatives sont souvent perçues comme une extension du gouvernement électronique, axé davantage sur la participation politique et les relations avec les acteurs non gouvernementaux, plutôt que sur une base théorique solide et un cadre stratégique.

1.3. Les bonnes pratiques de la gouvernance électronique

Les bonnes pratiques de la gouvernance électronique englobent plusieurs aspects essentiels pour garantir une gestion efficace des données et des services publics numériques, on peut citer :

1.3.1. Gouvernance politique

Une gouvernance politique efficace reconnaît le potentiel des données comme un outil puissant pour éclairer les décisions, Il est primordial de bénéficier d'un soutien politique solide de la part des responsables politiques pour garantir la cohérence et le développement des actions liées aux données. (Abylone, 2020).

1.3.2. Gouvernance territoriale

Considérer les données à l'échelle du territoire comme un atout stratégique pour le développement et la transformation en territoire intelligent est crucial. (Abylone, 2020).

1.3.3. Gouvernance technique

Mettre en place une infrastructure informatique robuste et adaptée pour fournir un catalogue de données aux acteurs publics du territoire est une pratique recommandée. **(Abylone, 2020).**

1.3.4. Formation et Sensibilisation

Promouvoir la maîtrise des technologies de l'information par toutes les catégories de la population et offrir une formation aux fonctionnaires et élus sur l'utilisation et la gestion des services de gouvernance électronique sont des actions importantes. (Le Conseil de l’Europe, 2004)

1.3.5. Confidentialité et Sécurité

Utiliser des méthodes d'authentification adaptées aux niveaux de confidentialité et de sécurité requis, ainsi que garantir le respect de la vie privée et la fiabilité des données personnelles, sont des aspects cruciaux à prendre en compte. (Le Conseil de l'Europe, 2004).

De plus, la sécurité de l'information requiert une expertise professionnelle, et les organisations doivent donc suivre les meilleures pratiques de leur secteur pour choisir les contrôles de sécurité appropriés. Le chiffrement est une mesure de sécurité efficace à cet égard. De plus, les entreprises et les organismes doivent se conformer à diverses normes nationales et internationales, telles que : (Baig.A, 2021)

-CENELEC - Comité européen de normalisation en électronique et en électrotechnique

Conseil des normes de sécurité PCI

-Les normes de l'Agence de l'Union européenne pour la cybersécurité (ENISA)

-Les normes de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

-Les normes ISO (ISO 27001, par exemple).

1.4. La gouvernance électronique au niveau international ; la Chine

La Chine s'engage activement dans la gouvernance électronique en mettant en place des réglementations et des structures pour superviser et protéger les données, ainsi qu'en cherchant à influencer la gouvernance d'Internet à l'échelle mondiale en promouvant son propre protocole d'adressage et en proposant des modifications pour façonner l'avenir d'Internet.

Le gouvernement chinois a dévoilé ses "directives pour renforcer la construction d'un gouvernement numérique", énonçant les objectifs de la Chine pour la transformation de son mode de gouvernance à l'ère du numérique d'ici à 2035.

Ce plan vise à renforcer la stabilité économique du pays en exploitant plus efficacement le big data, qui pourrait être utilisé pour renforcer les politiques de surveillance et de contrôle des citoyens.

La première étape de cette ambitieuse transformation numérique consiste à mettre en place un système qui exploite de manière plus efficiente les données. Sans entrer dans les détails, la Chine vise à atteindre cet objectif d'ici 2025, afin d'aider Pékin à élaborer une politique de gouvernance plus scientifique, précise et efficace en vue d'une meilleure gestion de son économie.

Le plan stipule que "la Chine renforcera l'intégration, la collecte et la gestion des données économiques pour développer des bases de données de gouvernance économique, et utilisera le big data pour améliorer l'analyse économique et détecter les risques potentiels".
En pratique, Pékin souhaite développer des outils de prédiction économique basés sur le big data, un concept déjà utilisé par l'OCDE pour des prévisions à court terme du PIB. Sous couvert de mesures de sécurité, la Chine affirme vouloir mettre en place un système de prévision et de prévention des risques en utilisant les données de sécurité publique, évoquant une perspective semblable au film "Minority Report".
En outre, Pékin envisage d'améliorer son programme "Sharp Eyes", un système de surveillance de masse visant à couvrir l'ensemble de l'espace public, selon le Centre de la sécurité et des technologies émergentes. (Mohr, Maxime, 2022).

1.5. La gouvernance électronique en Algérie

L'article de Hacene Derrar aborde la politique concrète adoptée par les autorités publiques pour favoriser la réussite de la transformation numérique en Algérie. Cette politique, qui positionne le numérique comme une priorité stratégique, s'est matérialisée à travers l'engagement n°25 du Président de la République visant à "réaliser une transformation numérique pour améliorer la connectivité, généraliser l'usage des TIC - notamment dans les administrations publiques - et améliorer la gouvernance économique". Cet engagement est appuyé par des orientations pratiques et opérationnelles du Président de la République, soulignant que la numérisation, au cœur de ses préoccupations, dépasse le simple aspect technique pour devenir une conviction profonde, élevée au rang de priorité pour la construction de la nouvelle Algérie. Cette vision confirme le rôle crucial que la transformation numérique devra jouer dans l'établissement d'un nouveau mode de gouvernance visant une croissance inclusive et génératrice d'emplois, en mettant en œuvre des moyens favorisant l'adaptation à un nouvel environnement économique et social.
Pour concrétiser cet engagement et ces orientations, le gouvernement a inclus dans son plan d'action plusieurs mesures visant en premier lieu la moralisation de la vie publique par la mise à disposition de données publiques, favorisant une plus grande transparence, responsabilité et efficacité de l'action publique. En plus des objectifs de transparence et d'efficacité visés, cette démarche vise également à créer les conditions nécessaires au développement d'une économie numérique reposant, entre autres, sur l'exploitation des données.
Ces actions ont pour objectif ultime de lutter contre la bureaucratie et de promouvoir la démocratie participative. Cela implique de promouvoir et de développer l'administration

numérique, tout en accélérant la dématérialisation des services publics, ce qui représente un excellent moyen d'accroître la transparence et d'améliorer l'efficacité et la proximité de l'action publique. Cela nécessite une refonte des modes de gestion de l'administration publique, exigeant impérativement la numérisation et la dématérialisation de divers services publics.

Ce nouveau mode de gouvernance, centré sur le développement de la numérisation, demande des infrastructures et solutions technologiques performantes, un secteur bancaire et financier moderne incluant une large adoption des instruments de paiement électronique, le développement du e-commerce, la digitalisation des opérations financières, ainsi que la modernisation et le renforcement des capacités de contrôle. Cela encourage l'émergence d'une économie nouvelle basée sur l'innovation, la compétitivité, la qualité et le savoir. (Derrar, Hacene, 2023).

L'Algérie a fait d'énormes progrès dans le domaine de la gouvernance électronique et de la participation citoyenne en ligne, comme le souligne une analyse du Groupement algérien des acteurs du numérique basée sur le dernier rapport des Nations Unies sur les e-gouvernements de 2022.

En ce qui concerne l'e-gouvernance, l'Algérie a progressé de 8 places depuis 2020, avec un indice de développement de l’e-gouvernement (EGDI) de 0,5611, la plaçant en 112 e position sur 193 pays et en 9 e position sur le continent africain. En ce qui concerne la participation électronique des citoyens, l'Algérie a fait un grand bond en avant en gagnant 35 places entre 2020 et 2022, bien qu'il reste encore beaucoup à faire pour progresser.

Malgré des améliorations, l'Algérie n'a pas encore atteint un niveau de performance optimal dans ce domaine, se situant à la 148e place sur 193 pays avec un indice de participation électronique (EPI) de 0,2273, ce qui est très en dessous de la moyenne mondiale et même africaine. (Rapport de l’ONU sur la gouvernance électronique)

2. La sécurité des données

2.1. Définition et concept

Avec le développement de l'Internet, l'informatique s'est basée essentiellement sur les communications entre serveurs, postes utilisateurs, réseaux et data center. Que ce soit pour externaliser le stockage des données à des fins de sauvegarde, utiliser des services logiciels hébergés ou recourir à la virtualisation chez un fournisseur tiers pour l'infrastructure informatique de l'entreprise, la sécurité des données revêt une importance cruciale. La sécurité des données implique l'utilisation de mesures de protection pour prévenir les accès

non autorisés, garantir la confidentialité, l'intégrité et la disponibilité des données. Les bonnes pratiques en matière de sécurité des données comprennent le chiffrement, la gestion des clés, la protection par occultation, la création de sous-ensembles de données, le masquage des données, ainsi que les contrôles d'accès et la surveillance des activités. (Rélaza, 2016)

Dans le domaine numérique, les objectifs de sécurité de l'information et de sécurité des données personnelles se rejoignent. Cette convergence a conduit à une interaction entre ces deux domaines, et à la création d'outils tels que les méthodologies d'évaluation des risques et les mesures de sécurité recommandées pour les personnes qui traitent et contrôlent les données. (Liem, C.; Petropoulos, G., 2016).

2.2. La sécurité des données et le Règlement Général sur la Protection des Données

Le RGPD, ou Règlement Général sur la Protection des Données, est un texte législatif adopté par le Parlement Européen et en vigueur depuis le 28 mai 2018. Son objectif principal est de renforcer la protection des données personnelles des citoyens de l'Union européenne en améliorant la transparence sur la collecte et l'utilisation de ces données. (CARPENTIER, Jean-François, 2023).

Selon la présentation de la CNIL (Commission Nationale de l'Informatique et des Libertés), le RGPD s'applique aux organismes collectant et traitant des données à caractère personnel des résidents de l'UE. Les entreprises clientes/utilisatrices d'un environnement Cloud restent responsables de la sécurité des données, même si elles externalisent le stockage ou le traitement de ces données à un fournisseur de services Cloud. (CARPENTIER, Jean-François, 2023).

La CNIL détaille également les différents principes du RGPD, qui sont les éléments clés du traitement des données, ainsi que le rôle de chaque acteur, comme le responsable de traitement et le délégué à la protection des données. (CARPENTIER, Jean-François, 2023).

L'augmentation de l'accessibilité des données personnelles soulève de nombreux risques, tels que l'atteinte à la vie privée, la commercialisation généralisée des données, le ciblage par les algorithmes, la falsification d'informations et la manipulation des faits. Le RGPD vise à établir un cadre légal européen pour la protection des données sensibles, telles que les données génétiques, biométriques et de santé. (Légifrance, 2018)

Selon le règlement général sur la protection des données (RGPD), les violations de données peuvent entraîner des amendes allant jusqu'à 4 % du chiffre d'affaires annuel mondial d'une entreprise. Les entreprises qui collectent et gèrent des données dans l'UE

doivent donc prendre en compte et gérer leurs pratiques de traitement des données pour se conformer aux exigences du RGPD. (Mesaros, Michael, 2020)

Le règlement général sur la protection des données concerne les entreprises qui manient les données de citoyens européens. Il leur donne de nouvelles obligations depuis mai 2018 :

✔ Recueillir un consentement explicite sur la collecte des données personnelles ;

✔ Appliquer le « Privacy by design », c'est-à-dire ne pas collecter de données sans qu'elles soient nécessaires au service rendu à l'utilisateur ;

✔ Droit à l'effacement des données sur demande de l'utilisateur ;

✔ Droit à la portabilité (réversibilité) des données sur demande de l'utilisateur ;

✔ Droit au refus du profilage automatique ;

✔ Notification en cas de fuite de données sous 72 heures.

En vertu du RGPD, les violations de données peuvent entraîner des amendes allant jusqu'à 4 % du chiffre d'affaires annuel mondial d'une entreprise. Les entreprises doivent donc respecter ces règles et adapter leurs pratiques de traitement des données en conséquence. (Plouin, Guillaume, 2022)

2.2.1. Sécurité des données

Les entreprises doivent mettre en place des mesures de sécurité adéquates, incluant des contrôles techniques et organisationnels, pour éviter les pertes de données, les fuites d'informations et toute opération de traitement de données non autorisée. Le RGPD encourage l'adoption de mesures telles que le chiffrement, la gestion des incidents, la protection du réseau et des systèmes, ainsi que la garantie de disponibilité et de résilience dans les programmes de sécurité des entreprises. (Mesaros, Michael, 2020)

2.2.2. Les droits étendus des particuliers

Les individus ont désormais plus de contrôle sur leurs données personnelles et bénéficient d'un ensemble de droits élargi en matière de protection des données. Cela inclut le droit à la portabilité des données et le droit à l'oubli, leur permettant ainsi de mieux gérer leurs informations personnelles. (Mesaros, Michael, 2020)

2.2.3. La notification de violation de données

Les entreprises doivent notifier aux autorités de régulation et/ou aux personnes concernées toute violation de données dès qu'elles en ont connaissance, dans un délai raisonnable. (Mesaros, Michael, 2020)

2.2.4. Les audits de sécurité

Les entreprises doivent documenter et maintenir à jour leurs pratiques de sécurité, évaluer régulièrement l'efficacité de leurs mesures de sécurité et ajuster leur approche si nécessaire. (Mesaros, Michael, 2020)

2.3. Modèles de sécurité des données

2.3.1. La triade Confidentiality, Integrity, Availability (CIA)

La triade CIA est un modèle de sécurité de l'information qui garantit la protection des données au sein d'une organisation ou d'une entreprise. Les trois principes fondamentaux de la confidentialité, de l'intégrité et de la disponibilité (Confidentiality, Integrity, Availability) forment la base d'une infrastructure sécurisée en matière de cybersécurité. Ces principes sont essentiels pour tout programme de sécurité, offrant aux entreprises une liste de contrôle simple mais complète pour évaluer leurs pratiques et leurs outils de sécurité.

Un système de sécurité de l'information doit impérativement respecter ces trois composantes pour être efficace. Tout manquement à l'un de ces aspects nécessite des corrections afin d'assurer la fiabilité du système. (Gastard, Richard, 2024).

2.3.2. Le modèle Authentication, Authorization, Accounting (AAA)

Le réseau AAA (Authentication, Authorization, Accounting) offre des services de contrôle d'accès à travers diverses technologies et plateformes réseau. Ces services se décomposent en trois points clés :

-L'authentification : Ce processus consiste à identifier une entité afin de décider si elle est autorisée à accéder à des ressources. Cela peut impliquer l'utilisation d'un nom d'utilisateur/mot de passe, d'une clé, de la reconnaissance biométrique, etc. Le serveur AAA compare les informations fournies avec celles enregistrées dans sa base de données d'utilisateurs pour valider les droits d'accès du client ;

-L'autorisation : Une fois l'authentification effectuée, ce service détermine les droits et les services que le client est autorisé à recevoir. L'authentification et l'autorisation sont généralement gérées par le même environnement de service AAA ;

-La comptabilité : Le réseau AAA propose des méthodes de collecte et d'envoi de données relatives à l'utilisateur. Cela permet notamment de générer des rapports, des factures et d'effectuer des audits. (P., Calhoun, 2001).

Un réseau AAA peut se résumer par le schéma suivant :

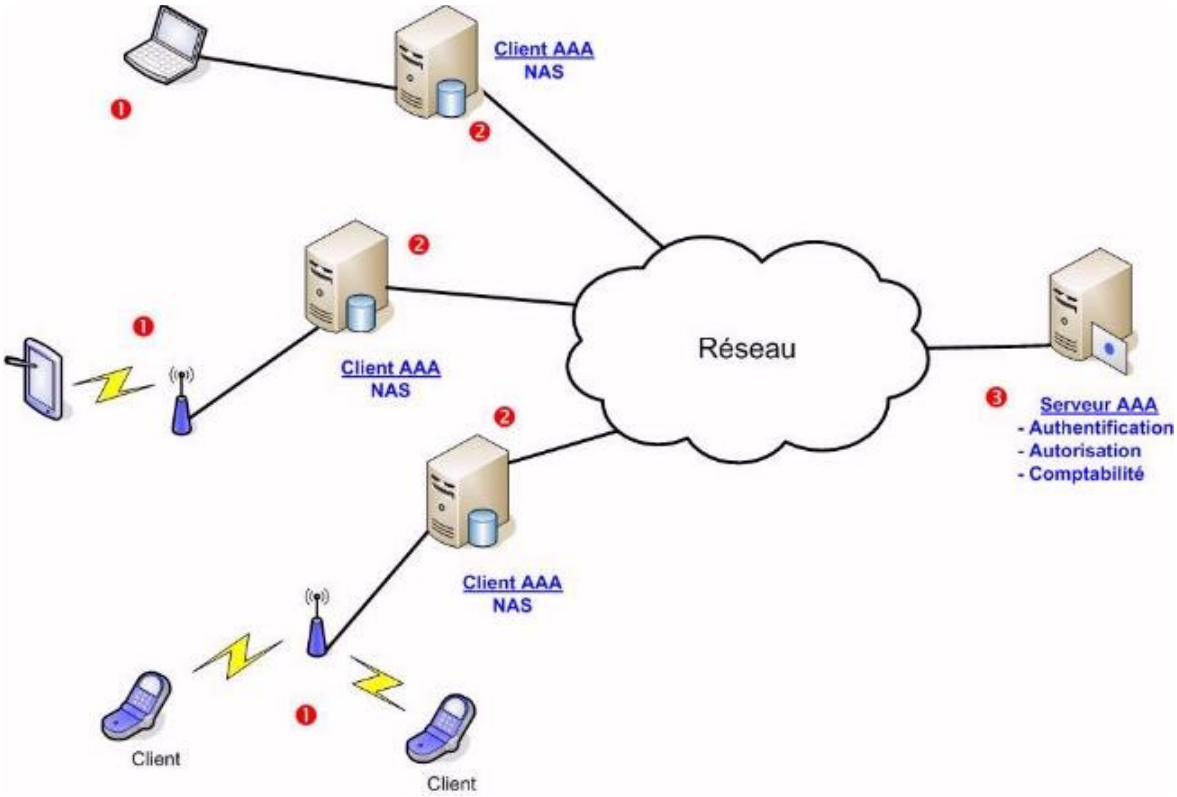


Figure 2 : schéma d'un réseau AAA.

Source : (P., Calhoun, 2001)

2.3.3. Le zéro trust

Créé par John Kindervag en 2010 lorsqu'il était analyste principal chez Forester Research, l'architecture Zéro Trust est une approche de sécurité qui vise à protéger efficacement les actifs critiques d'une organisation. Elle repose sur l'idée que chaque connexion et appareil du réseau sont potentiellement dangereux, qu'ils viennent de l'intérieur ou de l'extérieur. Le modèle Zéro Trust met en place des mesures pour contrer ces menaces en enregistrant et en inspectant tout le trafic réseau, en limitant et contrôlant l'accès au réseau, ainsi qu'en vérifiant et sécurisant les ressources.

Ce modèle garantit que les données et les ressources sont sécurisées par défaut, n'étant accessibles que de manière restreinte, dans des conditions spécifiques, suivant le principe d'accès au moindre privilège. Chaque connexion, que ce soit un utilisateur accédant à une application ou un appareil se connectant à un ensemble de données via une API, est vérifiée et autorisée selon les règles de sécurité de l'organisation. De plus, chaque appareil, flux réseau et connexion sont authentifiés et autorisés en fonction de règles dynamiques et du contexte provenant de multiples sources de données. (Lodewijkx, Koos, 2020)

2.4. Solutions de sécurité des données

2.4.1. Chiffrement des données

Le chiffrement est un mécanisme qui consiste à coder (ou brouiller) l'information. Le chiffrement des données peut être effectué à différents niveaux d'un système informatique, que ce soit au niveau d'un fichier individuel, d'une partition ou d'un disque complet. Il existe de nombreuses techniques de chiffrement qui ne seront pas détaillées ici.

Pour accéder aux données en clair, il est nécessaire de disposer de la clé de déchiffrement, le mot de passe étant la méthode la plus répandue.

Les mots de passe, bien que largement utilisés, ne sont pas suffisamment sécurisés ; il est recommandé de choisir des mots de passe robustes et de les stocker dans un gestionnaire de mots de passe. Les gestionnaires de mots de passe sécurisent les informations sensibles sous une forme chiffrée, accessibles uniquement avec les bonnes informations d'identification.

Les certificats, bien plus sûrs que les mots de passe, sont des documents numériques permettant de vérifier l'identité d'un utilisateur. Aujourd'hui, aucun système informatique sérieux ne devrait reposer uniquement sur des mots de passe.

En outre, il existe des techniques de chiffrement matériel qui peuvent être utilisées.

Quelle que soit la méthode de chiffrement choisie, il est essentiel de s'assurer qu'elle est adéquate pour répondre à vos besoins en termes de sécurité. (Centre canadien pour la cybersécurité, 2024).

Figure 3 : Représentation du chiffrement des données.

Source : (Centre canadien pour la cybersécurité, 2024).

2.4.2. Masquage des données

Le masquage des données consiste à créer des données fictives mais réalistes pour protéger les informations sensibles. Cette pratique est utilisée lorsque les données réelles ne sont pas nécessaires, comme dans les formations, les démonstrations commerciales ou les tests logiciels. Le processus de masquage des données implique la modification des valeurs tout en préservant le format, afin d'obtenir une version inexploitable ou rétrogradable.

L'anonymisation et le pseudo nymisation des données sont deux techniques très utiles. Les données pseudonymes permettent une certaine identification, tandis que les données anonymes empêchent toute possibilité de relier les informations à une personne spécifique.

La RGPD oblige les entreprises à supprimer les données personnelles non utilisées après un certain délai, mais ces données peuvent avoir une grande valeur. L'anonymisation permet de se conformer au RGPD tout en limitant la perte de valeur due à la suppression. (ITRex, 2023).

2.4.3. Prévention des fuites de données

La prévention des fuites de données (Data LeakPrevention, DLP) vise à empêcher la sortie de données sensibles de l'entreprise. Cette application met en place des règles pour détecter et bloquer le flux sortant potentiellement dangereux, comme les courriels envoyés en dehors de l'entreprise. En cas d'incident, elle alerte l'administrateur qui évalue la gravité de la situation.

Dans le cloud, on parle de CASB (Cloud Access Security Broker), une solution sécuritaire pour protéger les données stockées dans le cloud. Les CASB surveillent l'accès aux applications cloud, appliquent des politiques de sécurité pour préserver la confidentialité, l'intégrité et la disponibilité des données (Triade CIA). Ils offrent des fonctionnalités telles que la gestion des identités et des accès, le chiffrement des données, la détection des menaces, la prévention des fuites de données et la conformité réglementaire. (Leroy, Philippe, 2021)

2.5. Les problématiques de sécurité liées au cloud

Lorsque le concept de cloudcomputing est présenté à une personne non familière avec le sujet, sa première préoccupation tourne généralement autour de la confidentialité des données.

En effet, dans le monde de l'entreprise, il est largement ancré que les données informatiques doivent être conservées en interne pour garantir leur sécurité. Cette croyance peut sembler curieuse étant donné que les entreprises font déjà appel depuis de nombreuses années à des fournisseurs d'hébergement pour leurs applications web et leurs intranets

clients, avec parfois des données critiques concernant l'entreprise et sa clientèle transitant par ces tiers. (Plouin, Guillaume, 2022).

La confiance accordée à ces prestataires d'hébergement repose sur leur réputation sur le marché et sur les engagements contractuels qu'ils prennent. En effet, ils s'engagent légalement à respecter des "règles de confidentialité" interdisant la divulgation des données de leurs clients. Les fournisseurs de services cloud prennent des engagements similaires, mais ils suscitent parfois moins de confiance que les prestataires d'hébergement. Selon nous, cette méfiance est principalement due à l'origine du cloud : ces acteurs proviennent du monde du web, un domaine associé au grand public, tandis que les fournisseurs d'hébergement sont issus du secteur des télécommunications, un domaine traditionnellement associé aux entreprises.

La confidentialité des données hébergées chez l'opérateur cloud est en principe garantie contre le risque d'espionnage par les collaborateurs de l'opérateur grâce à :

- Le contrat établi entre l'entreprise utilisatrice et l'opérateur ;
- Les certifications obtenues par l'opérateur.

Ces garanties peuvent être considérées comme adéquates ou non en fonction des circonstances. Par exemple, une entreprise détenant des secrets industriels pourrait hésiter à les stocker dans le cloud. Afin de rassurer leurs clients face à la surveillance potentielle par des entités telles que la NSA, plusieurs acteurs du cloud chiffrent leurs données. Certains grands acteurs offrent même la possibilité du "bringyourownkey", où la clé de déchiffrement des données est conservée dans l'entreprise, et pas dans le cloud. Il est même possible de chiffrer les données en mémoire vive. (Plouin, Guillaume, 2022).

2.5.1. La confidentialité des données transitant sur le réseau

Elle est généralement assurée par les opérateurs cloud via l'utilisation systématique du protocole SSL pour garantir la confidentialité des échanges de données. Ce protocole offre un niveau de sécurité adéquat. Certains grands opérateurs cloud tels qu'Amazon, Google ou Microsoft vont encore plus loin en proposant un chiffrement IPSEC ou une liaison dédiée entre leur Datacenter et le système d'information, offrant ainsi un niveau de sécurité encore plus élevé. Pour renforcer la protection contre l'espionnage, plusieurs acteurs du cloud chiffrent désormais les échanges de données au sein de leur propre réseau interne. (Plouin, Guillaume, 2022)

2.5.2. Un avantage du cloud

Lorsqu'une entreprise gère ses serveurs sur son réseau informatique. Dans ce cas, il est fréquent de devoir gérer plusieurs scénarios d'accès, notamment des utilisateurs accédant aux applications depuis le siège, un site secondaire ou en situation de nomadisme. Les responsables réseau doivent ainsi gérer divers scénarios de sécurité, incluant l'authentification et le chiffrement en fonction de ces différentes populations : des accès directs pour les utilisateurs du siège, des connexions VPN (Réseau Privé Virtuel) pour les utilisateurs du site distant, et des serveurs mandataires inverses (Reverse Proxy) pour les utilisateurs nomades. (Plouin, Guillaume, 2022)

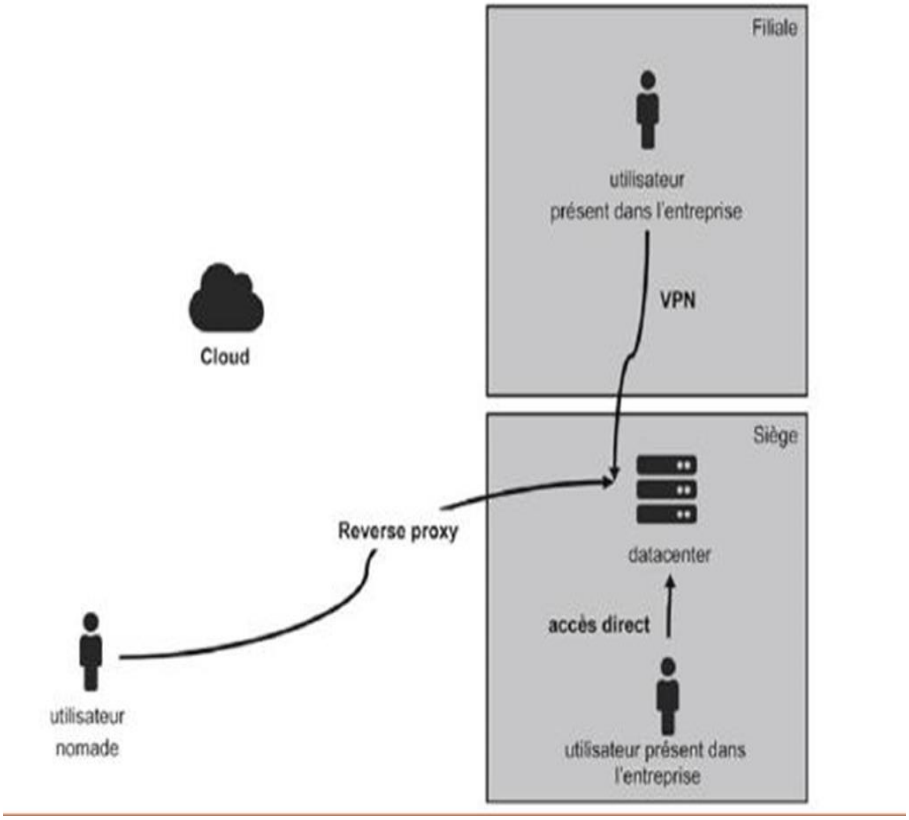


Figure 4 : Variétés des accès en entreprise et problématiques de sécurité.

Source : (Plouin, Guillaume, 2022).

Section 3 : la gouvernance électronique et la sécurité des données

1. La gouvernance électronique des données comme levier de sécurité

La gouvernance électronique des données et la sécurité des données sont étroitement liées. La gouvernance des données, en mettant en place des rôles, des processus et des règles spécifiques, assure une utilisation optimale des actifs de données tout en garantissant leur protection et leur sécurité.

Elle englobe la gestion des données, la promotion de l'adhésion des parties prenantes aux politiques de l'organisation, et la définition de rôles et responsabilités pour assurer une utilisation efficace, sécurisée et responsable des données. D'autre part, la sécurité des données vise à protéger les informations sensibles contre les menaces telles que les vols de données et les malwares, assurant la confidentialité, l'intégrité et la disponibilité des données.

Une stratégie de sécurité efficace est essentielle pour se conformer aux réglementations en matière de protection des données, éviter les violations de données et protéger la réputation et les actifs d'une entreprise. (LADJIMI, Chokri; MENICACCI, Alexandre).

2. Gouvernance électronique et sécurité des données ; les tendances actuelles et les défis futurs

La gouvernance électronique des données et la sécurité des données sont des aspects essentiels dans le contexte numérique actuel, avec des tendances et des défis significatifs à prendre en compte.

2.1. Tendances actuelles

- L'importance de la gouvernance des données : elle permet une gestion optimale des actifs de données en établissant des rôles, des processus et des règles spécifiques ;

-Stratégie de sécurité des données : une stratégie de sécurité efficace garantit la confidentialité, l'intégrité et la disponibilité des données, tout en assurant la conformité aux réglementations en matière de protection des données ;

-Réglementations sur la protection des données : de nombreux pays ont mis en place des réglementations telles que le RGPD, le CCPA, le HIPAA, etc., pour encadrer la protection des données. (Galvez, Rachel, 2024)

2.2. Défis futurs

Comme pour toute nouvelle initiative, la mise en œuvre d'une stratégie de gouvernance des données comporte des défis.

-Contraintes liées aux ressources : Les petites et moyennes entreprises rencontrent des difficultés pour recruter localement des professionnels qualifiés capables de mettre en place un plan de gouvernance des données. Les administrateurs actuels sont déjà débordés par leurs tâches et ne disposent pas du temps nécessaire pour assumer une nouvelle responsabilité. Même avec l'automatisation, il est essentiel d'avoir les bonnes compétences pour la conception et le déploiement, ce qui conduit de nombreuses organisations à avoir recours à un aide extérieur pour démarrer ;

-Silos de données : Les changements technologiques fréquents, l'ajout de nouvelles technologies, les difficultés de communication et le roulement constant du personnel entraînent une dispersion des données dans des endroits spécifiques au sein des petites entreprises ;

-Manque de leadership : Même les employés familiarisés avec la gouvernance des données nécessitent une direction et un leadership clairs pour sa mise en œuvre. Un bon leader informera et guidera les utilisateurs tout au long de la stratégie de gouvernance des données, de sa conception jusqu'à sa réalisation ;

-Adoption du cloud : l'adoption du cloudcomputing présente des défis tels que le manque de compétences, les investissements préexistants dans les Datacenter, et l'enfermement propriétaire, nécessitant une formation et une compréhension approfondie avant la migration vers le cloud ;

-Gouvernance des données dans le cloud : la gouvernance des données dans le cloud pose des défis en matière de sécurité des informations et de conformité aux réglementations, nécessitant une compréhension des besoins de l'entreprise et des réglementations en vigueur ;

-Sécurité du cloud : les défis de la sécurité du cloud incluent les compromissions de données et la vulnérabilité des systèmes, mettant en lumière l'importance de développer des stratégies de sécurité solides pour protéger les données ;

-Exigences commerciales définies : La première étape pour établir des politiques de données consiste à comprendre les besoins de l'entreprise. Cela implique la création de cas d'utilisation et une compréhension approfondie de l'utilisation des données à travers toute l'organisation ;

-Qualité des données : Des données de qualité médiocre compliquent l'amélioration de l'intégrité des données et la détermination de la responsabilité. Il est parfois essentiel d'organiser et d'améliorer les données avant d'envisager la mise en place d'un plan de gouvernance des données ;

-Manque de contrôle : Dans les petites structures, la gestion des données peut être défaillante, les données étant dispersées à travers toute l'organisation. Cela entraîne un manque de contrôle global sur l'ensemble des données, pouvant ainsi causer des lacunes lors d'éventuels audits. (Groeneveld, Rachid, 2021)

3. Les enjeux de la gouvernance électronique des données pour la sécurité des systèmes d'information ; état des lieux et recommandations

3.1. Enjeux de la Gouvernance Électronique des Données

La protection des actifs informationnels est d'une importance primordiale pour les organisations, qui sont confrontées à des menaces telles que les fuites de données, les cybers attaques et le vol d'équipements informatiques professionnels.

Les entreprises reposent sur les systèmes d'information pour stocker des données sensibles et sécuriser leur propriété intellectuelle, mettant en évidence l'importance cruciale de la sécurité des SI pour maintenir la confiance et la réputation des clients. Voici quelques-uns des principaux enjeux :

-Ne pas perdre d'information : Les entreprises cherchent à éviter la perte d'informations essentielles pour leur pérennité, telles que les brevets, les contrats clients ou les litiges, en mettant en place une gestion documentaire efficace. (Abylone, 2020)

-Garantir son accessibilité : Assurer la disponibilité des informations et faciliter leur partage pour optimiser la collaboration représente la principale exigence des entreprises en matière de gestion documentaire. (SERDALAB, 2014)

-Le risque juridique : En ce qui concerne le respect des exigences réglementaires, la démarche est similaire. Les entreprises sont tenues de se conformer à des normes et réglementations de plus en plus strictes, ainsi qu'à des normes de transparence financière qui soulèvent la question de la conservation à long terme des documents. Le nombre d'autorités établissant des règlements et des sanctions a également augmenté. Les entreprises accordent de plus en plus d'importance à garantir la traçabilité des documents afin de prouver leur conformité. (OUDIPO, 2014)

-Conserver son savoir et son savoir-faire : La notion de mémoire organisationnelle est apparue aux États-Unis dans les années 1990. Les dirigeants ont pris conscience que le savoir-faire et les connaissances sont des ressources essentielles pour l'entreprise. Enregistrer ces connaissances et les diffuser de manière organisée contribue à la performance globale de l'entreprise. Ainsi, l'entreprise peut :

- Faciliter le transfert des connaissances ;
- Accroître la productivité ;
- Favoriser l'innovation ;
- Construire un patrimoine immatériel. (Brigitte, 2013)

-Conserver sa réputation : Une gestion inadéquate de l'information peut avoir un impact sur l'image de l'entreprise à deux niveaux. En interne, cela peut entraîner des risques psycho-sociaux. En externe, une diffusion inadéquate de documents confidentiels peut ternir sa réputation. Ainsi, les entreprises s'efforcent d'améliorer la protection de leurs informations pour prévenir de tels risques et préserver leur image. (BLANGER Jean-Pierre, 2013).

-Economiser : Une augmentation de la productivité et de la sécurité contribue aux bénéfices financiers d'une entreprise. En revanche, les arrêts de production, les rappels dans l'industrie, et les accidents entraînent des coûts financiers élevés ainsi qu'une atteinte à l'image de la société. Le coût des sanctions et des litiges est bien plus élevé que celui lié à la mise en place d'une politique efficace.

Les organisations se préoccupent de plus en plus de réaliser des économies en matière de développement durable. Réduire les impressions, les redondances et les copies de documents contribue à cet objectif, tout comme la réduction et la mutualisation des ressources documentaires.

Par ailleurs, les entreprises accordent une attention croissante à la réduction des coûts de stockage informatique pour réaliser des économies. Les capacités de stockage augmentent à des coûts moindres. Cependant, la quantité de données augmente plus rapidement que la baisse des coûts de stockage. (BLANGER Jean-Pierre, 2013).

3.2. Le rôle clé de la gouvernance électronique dans la protection des données

La gouvernance électronique revêt une importance cruciale dans la gestion de la sécurité des données numériques. Elle vise à mettre en place un cadre robuste de politiques, processus et contrôles afin de protéger les informations contre les menaces émergentes telles que les cyberattaques, les fuites de données et les accès non autorisés (Boughzala, I.; Bououd, I.; Michel, H., 2015). Trois principes fondamentaux sous-tendent la sécurité des

données dans le cadre de la gouvernance électronique : la confidentialité, l'intégrité et la disponibilité. (Triandis, A.; Williams, R. L., 2020).

Pour assurer la confidentialité, des mesures strictes régissent l'accès aux informations sensibles. L'utilisation de techniques avancées telles que le chiffrement des données et l'authentification multi facteur permet de restreindre l'accès aux seules parties autorisées (Kshetri, 2017). L'intégrité des données est préservée en détectant et prévenant toute altération non autorisée. Des contrôles rigoureux sont mis en place pour auditer les modifications et s'assurer que seules les entités habilitées peuvent apporter des changements (Boughzala, I.; Bououd, I.; Michel, H., 2015). Quant à la disponibilité, elle est garantie par des mécanismes visant à éviter les interruptions de service et à assurer l'accessibilité des données en temps voulu. Cela implique notamment la mise en œuvre de sauvegardes régulières et de plans de reprise après sinistre (Triandis, A.; Williams, R. L., 2020).

Dans le contexte actuel de la transformation numérique et de l'accumulation massive de données à caractère personnel, la gouvernance des données devient essentielle (Milos Brkovic, 2022). Les organisations se doivent de définir une stratégie claire de protection des données, alignée sur les risques et les exigences réglementaires en vigueur (Chen, J. V.; Distler, F., 2019). La gouvernance électronique, en encadrant rigoureusement la sécurité des données, contribue ainsi à préserver la confiance numérique et à favoriser l'adoption sécurisée des nouvelles technologies.

CHAPITRE II : CADRE METHODOLOGIQUE

Section 1 : Méthode

Ci-après, nous allons évoquer l'approche méthodologique choisie pour mener notre étude, nous présenterons ainsi les méthodes et instruments de collecte de données ainsi que la méthode d'échantillonnage, puis les méthodes d'analyses et traitement des données

1. Champ épistémologique de la recherche

Dans le contexte des différentes approches de recherche scientifique, il est important de situer cette étude dans un paradigme épistémologique approprié. Cela permettra de développer une méthodologie cohérente avec cette approche spécifique (Gavard-Perret, M.-L.; Gotteland, D.; Haon, C.; Jolibert, A., 2012).

L'épistémologie peut être définie comme l'étude de la manière dont les connaissances valables sont formées (Piaget J., 1967).

On peut distinguer les différents paradigmes épistémologiques sur un continuum allant d'une réponse essentialiste à une réponse non essentialiste à cette question :

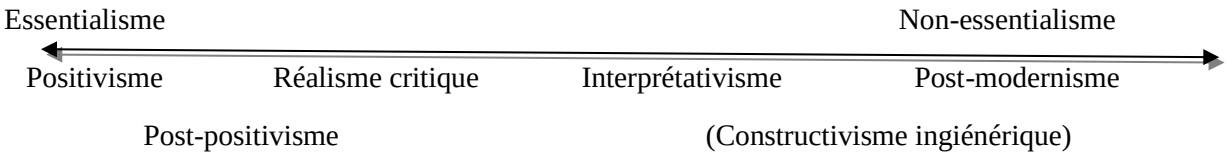


Figure 5 : Conception du réel et paradigmes épistémologiques.

Source : (Gavard-Perret, M.-L.; Gotteland, D.; Haon, C.; Jolibert, A., 2012).

D'après les fondements de l'épistémologie de la recherche scientifique, Le positivisme soutient que la réalité est régie par des lois immuables et presque toujours constantes, ce qui en fait un univers structuré de manière fixe. » (Kremer-Marietti A., 1993), les paradigmes du constructivisme partagent une méfiance envers toute idée d'une réalité essentielle, mettant en avant la particularité des réalités qui les composent. Pour Passeron, les normes, les valeurs, les conventions et les idéologies sont contingentes, situées historiquement et spatialement, ce que souligne (Lyotard J.-F., 1995) en affirmant que les réalités humaines et sociales sont spécifiques en raison de leurs dimensions intentionnelles, signifiantes et symboliques.

Cette recherche repose sur l'idée d'une réalité observable et mesurable, avec une base dans l'objectivité du chercheur. Cependant, cette réalité n'est pas considérée comme absolue, car les résultats de la recherche peuvent comporter une certaine marge d'erreur. Ainsi, cette approche s'inscrit dans le cadre du réalisme critique.

En outre, cette recherche repose sur l'interprétation des données fournies par les individus étudiés. Ainsi, elle se situe entre l'approche positiviste et interprétative, adoptant une posture post-positiviste et utilisant des méthodes quantitatives.

Dans l'approche post-positiviste, on cherche à vérifier le modèle d'analyse et à répondre à la question posée en utilisant une démarche hypothético-déductive pour tester les hypothèses. Cette réflexion confronte un ensemble de connaissances théoriques à la réalité pour en tirer des conclusions. (Poussing, Nicolas; Dagorn, Nathalie, 2012).

2. Méthode d'analyse

Compte tenu de l'objectif principal de l'étude à savoir mesurer l'impact de la gouvernance électronique des données sur la sécurité des données, et des recherches effectuées sur la thématique de notre sujet et vu la nature de nos variables notamment la gouvernance électronique des données, la sécurité des données.

La revue de littérature fournit des explications sur le cadre méthodologique utilisé. Cette recherche associe un raisonnement logique à des éléments empiriques, et le choix de la méthode d'analyse se porte sur une approche quantitative. Cette méthode est considérée comme plus appropriée pour tester les hypothèses et répondre à la question de recherche. (Poussing, Nicolas; Dagorn, Nathalie, 2012).

Les données sont collectées sur le terrain en administrant un questionnaire de recherche via Google Forms. Cette méthode permet de recueillir un grand nombre de données pour étudier un échantillon de grande taille.

Les résultats présentés dans la section suivante sont basés sur des analyses statistiques qui permettent d'examiner les relations entre les données et d'évaluer leur signification. L'analyse est menée à deux niveaux. Tout d'abord, les statistiques descriptives sont utilisées pour réaliser une analyse unidimensionnelle visant à obtenir des résultats descriptifs de l'échantillon étudié, Une analyse bidimensionnelle est utilisée par la suite, afin de déterminer la relation entre les variables.

2.1. Questionnaire de recherche

Une fois que la problématique de la recherche et les objectifs sont clairement définis, il est important de déterminer les dimensions à explorer pour répondre à cette question. Ces dimensions, représentées par des variables, utilisent des indicateurs pour la mesure et l'évaluation, qui sont définis en se basant sur la littérature existante. (Poussing, Nicolas; Dagorn, Nathalie, 2012).

2.1.1. Construction du questionnaire

La création des questions, des échelles et des autres composantes du questionnaire a été influencée par une analyse minutieuse de la littérature existante ainsi que par les recommandations d'experts dans le domaine.

Le questionnaire, dans sa section 2, accorde une attention particulière à l'évaluation des connaissances relatives à la gouvernance électronique et à la sécurité des données. Cette approche trouve un écho dans les travaux de (Poussing, Nicolas; Dagorn, Nathalie, 2012). (1.3), ainsi que ceux de (Ullah, F.; Sepasgozar, S. M.; Wang, C., 2019) (1.8) issus de la revue de littérature, qui mettent en exergue l'importance cruciale de la sensibilisation et de la formation sur ces thématiques.

De surcroît, cette même section du questionnaire met l'accent sur la perception de la conformité aux réglementations en matière de protection des données personnelles. Cet aspect revêt une importance capitale dans les études de (Franco, Jean-Michel, 2018) (1.5) et de (Tomo, A.; Todisco, M.; Ruggieri, M.; Vinci, M. B., 2021) (1.10), lesquelles soulignent le rôle prépondérant de la gouvernance des données dans l'assurance de cette conformité réglementaire.

Par ailleurs, les mesures de sécurité et les pratiques de gouvernance électronique font l'objet d'un examen approfondi à la fois dans la section 3 du questionnaire et dans plusieurs contributions de la revue de littérature, notamment les articles de (Zissis, D.; Lekkas, D., 2012) (1.7), (Aloufi, A. A.; Vasarhelyi, M. A., 2022) (1.9), ainsi que (Ullah, F.; Sepasgozar, S. M.; Wang, C., 2019) (1.8). Ces travaux approfondissent les mesures de sécurité, les contrôles et les politiques à mettre en œuvre dans le cadre de la gouvernance électronique afin d'assurer une protection optimale des données.

Cette analyse comparative met en lumière les convergences notables entre le questionnaire et la revue de littérature, témoignant d'une préoccupation partagée pour l'évaluation des connaissances, la conformité réglementaire et les mesures de sécurité dans le contexte de la gouvernance électronique et de la protection des données.

Dans le but de simplifier le traitement des données, les questions posées sont fermées, la plupart étant à choix unique ou multiples. De plus, les variables sont mesurées à l'aide d'échelles, avec une préférence pour l'échelle de Likert à 5 points en raison de sa praticité et de son utilisation répandue. Cette méthode est maintenue tout au long du questionnaire pour assurer la cohérence.

Dans le but de rendre les réponses plus rapides, des questions filtres sont mises en place avant chaque section. La première question filtre permet de vérifier si le répondant est admissible à l'enquête. Après avoir effectué un test-pilote, on estime qu'il faudra en moyenne de 7 à 10 minutes pour répondre au questionnaire.

2.1.2. Structure du questionnaire

Le questionnaire construit pour cette étude est composé de 20 questions structurées, regroupées en 3 grandes sections. Chaque section constitue les indicateurs de mesure d'une variable, et ainsi précédée d'une question filtre afin de différencier les personnes concernées. Le questionnaire est constitué ainsi :

- Fiche signalétique ;
- Connaissances générales sur la gouvernance électronique et la sécurité des données ;
- Mesures de sécurités et pratiques de gouvernance électronique.

Notre questionnaire contient plusieurs types de questions dont :

- ✓ Des questions dichotomiques se composent de deux propositions et une seule réponse est acceptée, généralement elles sont des affirmations ou des négations ;
- ✓ Des questions à choix unique se composent de plusieurs propositions et une seule réponse est acceptée ;
- ✓ Des questions à choix multiple se composent de plusieurs propositions et plusieurs réponses sont acceptées. ;
- ✓ Des questions ouvertes ;
- ✓ D'échelle de Likert contient un ensemble des questions de proposition auxquelles nous devons mesurer selon cinq échelons. Dans notre étude, nous appliquons ce type dans la question n°4 et la question n°11 sur un échelon de cinq de « très insatisfait » jusqu'à « Très satisfait ».

En résumé, le questionnaire employé dans notre étude a été méticuleusement élaboré afin d'appréhender de manière approfondie l'influence de la gouvernance électronique sur la sécurité des données chez les employés d'Algérie Télécom. Ceci vise à obtenir des réponses précises et exhaustives à notre problématique de recherche, en tenant compte des divers aspects de l'étude.

2.1.3. Validation du questionnaire

Avant de diffuser le questionnaire à l'ensemble des participants, une phase de pré-test est menée auprès d'un petit groupe représentatif. Ce pré-test permet de valider le contenu du questionnaire et de s'assurer que les questions correspondent aux objectifs de l'étude. Il permet également de vérifier la clarté et la compréhension des questions, afin d'éviter toute

ambiguïté.

Suite à l'analyse des réponses recueillies lors du pré-test, des modifications ont été apportées au questionnaire. Certaines questions ont été reformulées, d'autres ont été ajoutées. Ces ajustements visent à améliorer le questionnaire et à obtenir une version finale qui sera distribuée à l'ensemble de la population cible.

2.2. La méthodologie de traitement des données

2.2.1. Test de fiabilité

Avant d'analyser les données des clients, on présente le tableau des statistiques de fiabilités qui nous donne des résultats de Coefficient de Fiabilité (Alpha Cronbach) qui mesure la fiabilité entre les variables. Alpha Cronbach est l'un des tests statistiques les plus importants pour analyser les données d'un questionnaire, afin de lui conférer une légitimité. À la lumière des résultats de ce test, le questionnaire sera modifié ou accepté. Ce test est utilisé pour déterminer si les questions du questionnaire sont cohérentes les unes avec les autres.

Tableau 1 : statistiques de fiabilités.

	Nombre d'éléments	Coefficient de Alpha Cronbach
Connaissances générales sur la gouvernance électronique et la sécurité des données.	6	0.615
Mesures de sécurité et pratiques de gouvernance électronique.	16	0.771
Total	22	0.886

Source : Établi par nous-mêmes sur la base des résultats sur spss.

La valeur du coefficient de fiabilité est entre (0) et (1), la valeur est acceptable à partir du 0.60. Nous notons que le coefficient alpha Cronbach total est de 0.886 (supérieur à 0.60) ce qui indique qu'il existe une forte corrélation entre les variables, ce qui nous permet de confirmer la fiabilité du questionnaire de notre étude.

2.2.2. Les étapes du traitement statistique des données

Le traitement des données est une étape très importante car elle nous permet d'analyser les réponses obtenues. Pour avoir les tableaux les statistiques et les graphes nous passons par les étapes suivantes :

• Télécharger les résultats du formulaire électronique directement à partir du « Google Forms », et grâce à « Google Sheets » nous l'avons stocké facilement sous forme d'un

fichier Excel pour effectuer les opérations nécessaires en attribuant des codes à toutes les réponses pour faciliter le processus de décompression dans le logiciel Spss ;

• Créer un fichier spécial pour les résultats de l'étude dans le logiciel Spss et définir les questions et déterminer leurs types ainsi que le code accordé aux réponses ;

• Transférer et copier les réponses directement d'Excel vers Spss ;

• Analyser les réponses sur Spss.

2.2.3. Méthodes de traitement statistique

Dans le but d'analyser les données de l'échantillon, le programme Statistical Package for Social Sciences (SPSS) a été utilisé. Parmi les méthodes de traitement statistique les plus importantes utilisées dans cette étude, on trouve les suivantes :

- Fréquences et pourcentages : Les fréquences et pourcentages ont été utilisés pour décrire les caractéristiques de l'échantillon de recherche, et pour déterminer les réponses de ses membres concernant les différents axes de recherche ;

- Moyenne arithmétique : Elle est utilisée pour déterminer l'importance relative des réponses des répondants par rapport aux axes de l'outil d'étude. La moyenne arithmétique est utilisée pour classer les réponses des répondants selon le degré d'accord et pour savoir dans quelle mesure les opinions des individus sont élevées ou faibles sur chacune des affirmations des axes du questionnaire ;

- Écart-type : Il a été utilisé pour identifier l'étendue de l'écart des réponses des individus de l'étude par rapport à chaque affirmation, ainsi que la dispersion des réponses des membres de l'échantillon, plus sa valeur est proche de zéro, cela signifie que les réponses sont concentrées et non dispersées ;

- Coefficient alpha de Cronbach : Il a été utilisé pour déterminer la stabilité des affirmations du questionnaire, de sorte qu'il prend des valeurs allant de 0 à 1. S'il n'y a pas de stabilité complète dans les données, la valeur du coefficient est égale à zéro, mais s'il y a une stabilité complète dans les données, alors la valeur du coefficient est égale à un, ce qui signifie qu'une augmentation de la valeur de ce coefficient signifie une augmentation de la crédibilité des données ;

- Coefficient de corrélation de Pearson : Il est utilisé pour mesurer la validité de la cohérence interne de chaque affirmation du questionnaire avec l'axe auquel cette affirmation appartient ;

- Test de régression linéaire simple et multiple : Il est basé sur l'étude de deux variables, l'une étant indépendante et l'autre étant une variable dépendante, afin de trouver une relation entre ces deux variables. Il aide également à expliquer le changement qui peut se

produire dans la variable dépendante en fonction de la variable indépendante, puis à répondre aux hypothèses de l'étude.

Section 2 : Données

Il convient de souligner que l'objectif de cette étude est d'évaluer l'impact de la gouvernance électronique des données sur la sécurité des données. Nous allons maintenant présenter dans cette partie la population et l'échantillon de notre étude ainsi que les variables de mesures.

1. Population et données

1.1. Population cible

La sélection de la population étudiée découle d'une évaluation approfondie de la littérature dans le but d'assurer la fiabilité et la généralisation des résultats.

Cette enquête aspire à fournir des informations précieuses pour renforcer la protection des données au sein d'Algérie Telecom. L'unité statistique de notre étude comprend les employés d'Algérie Telecom, avec un nombre total de 286 employés, en raison de leur expérience et de leur exposition directe aux systèmes de gestion de l'information et de sécurité des données.

1.2. Choix de l'échantillon

Nous avons choisi d'utiliser une méthode d'échantillonnage non probabiliste pour la collecte de données. La méthode d'échantillonnage quantitative vise à minimiser les biais et à assurer la représentativité des échantillons pour obtenir des résultats fiables et significatifs.

1.3. Taille de l'échantillon

Pour déterminer la taille de notre échantillon, nous avons consulté la littérature scientifique ainsi que des experts du domaine qui ont mené des études similaires.

En appliquant la formule de calcul de l'échantillon, nous avons obtenu le résultat ci-dessous :

$$n = \frac{\frac{z^2 \times p(1-p)}{e^2}}{1 + \left(\frac{z^2 \times p(1-p)}{e^2 N}\right)}$$

Avec :

- ✓ n = taille de l'échantillon à étudier ;
- ✓ N= taille de la population mère ;

- ✓ e = marge d’erreur ;
- ✓ p = proportion (homogénéité de la population) ;
- ✓ z = cote z (du niveau de confiance).

Nous avons utilisé une proportion de 0.5 (car nous ne connaissons pas l’homogénéité de notre population), un niveau de confiance de 95 % (cote z = 1,96) et une marge d’erreur de 6.8 %.

Sur la base de nos calculs, nous avons choisi un échantillon de 120 employés.

1.4. Collecte de données

Le questionnaire a été créé à l'aide de la plateforme Google Forms et diffusé aux employés d’Algérie Telecom ; des exemplaires ont également été imprimés et remis aux employés pour qu'ils puissent y répondre.

2. Période de l’enquête

Le recueil de données s’étend sur une période de 9 jours allant entre le 28 avril 2024 et le 05 mai 2024. En premier lieu, l’enquête est réalisée en repérant les employés d’Algérie Telecom.

3. Variable de mesure

L'enquête se base sur un ensemble de variables qui sont définies dans le questionnaire à partir de la revue de littérature. Ces variables sont ensuite évaluées à l'aide d'indicateurs de mesure. Les variables de l'analyse et leurs indicateurs sont présentés ci-dessous.

3.1. Variable dépendante

La sécurité des données : est un aspect central de la protection des données. Les responsables du traitement des données et les sous-traitants doivent prendre les mesures appropriées pour éviter toute violation de la sécurité des données. (Meyer & Davies, 2023)

3.2. Variables indépendantes

La gouvernance électronique : La gouvernance électronique fait référence à l'utilisation des technologies de l'information et de la communication (TIC) par les organismes gouvernementaux pour fournir des services publics de manière plus efficace et transparente. Elle englobe des aspects tels que les politiques, les processus, les normes et les réglementations encadrant la gestion et la protection des données (Ndou, 2004).

Section 3 : Présentation de l'entreprise

Algérie Télécom est en tête sur le marché des télécommunications en Algérie, un secteur en pleine expansion, en proposant une variété de services de téléphonie fixe et d'accès à internet à une clientèle diversifiée, tant résidentielle que professionnelle. Sa position dominante découle d'une stratégie innovante axée sur les besoins des clients et sur l'évolution des usages, ce qui lui permet de se démarquer et de répondre efficacement aux attentes du marché.

Algérie Télécom est une société publique présidé par Monsieur Adel BENTOUMI avec un nombre totale de 21408 employés, opère dans le secteur des télécommunications, de la téléphonie fixe et d'internet. Son siège social est sis à la route nationale N°5 cinq maisons El Harrach Alger. Sa création a été officialisée par la loi 2000/03 du 5 août 2000, qui vise à restructurer le secteur des Postes et Télécommunications en séparant les activités postales de celles des télécommunications. Cette loi établit également les règles générales régissant la poste et les télécommunications, ainsi que les décisions du Conseil National des Participations de l'État (CNPE) du 1er mars 2001 qui instituent une Entreprise Publique Économique appelée "Algérie Télécom".

Cette loi accorde à Algérie Télécom le statut d'une entreprise publique économique sous forme de société par actions SPA, avec un capital social de 115.000.000.000,00 Dinars. La société a été enregistrée au centre national du registre de commerce le 11 mai 2002 sous le numéro 02B 0018083.

Entrée officiellement en activité à partir du 1er janvier 2003, elle s'engage dans le monde des Technologies de l'Information et de la Communication avec trois objectifs :

- Rentabilité
- Efficacité
- Qualité de service

Avec le slogan "Toujours Plus Proche", Algérie Télécom s'engage à se rapprocher des résidents algériens, où qu'ils se trouvent. En s'impliquant dans une expansion continue, notamment par l'extension de son infrastructure et sa mise à jour technologique, Algérie Télécom propose une variété de produits et services à sa clientèle, tout en contribuant à la croissance économique de la nation.

1. Algérie Télécom en Chiffres

Tableau 2 : Algérie Télécom en Chiffres.

Agences commerciales labélisées FI KHIDMATIKOM.	**91 %** des sites d'accueillabélisés.
Clients raccordés à Internet	Plus de **5.6M** Clients
Clients raccordés en Fibre optique	Plus de **1.2M** Clients
Clients raccordés en ADSL/VDSL	Plus de **2.7M** Clients
Clients Idoom 4G	Plus de **1.7M** Clients
Réseau commercial	**Plus de 500** Agences et points de présence

Source : à partir des documents internes de l'entreprise**.**

2. Organigramme d'Algérie Télécom

Voir annexe B.

CHAPITRE III : RÉSULTATS ET DISCUSSION

Le chapitre qui suit expose les résultats de l'étude quantitative, qui seront ensuite discutés dans la partie suivante.

Section 1 : Présentation, analyse et interprétation des résultats

1. Analyse descriptive des réponses des interrogés

Question : Vous êtes ? :

Tableau 3 : la répartition des interrogés selon le genre.

Variable	Fréquence	%
Homme	56	46.7
Femme	64	53.3
Totale	120	100.0

Source : Établi par nous-mêmes sur la base des résultats sur spss.

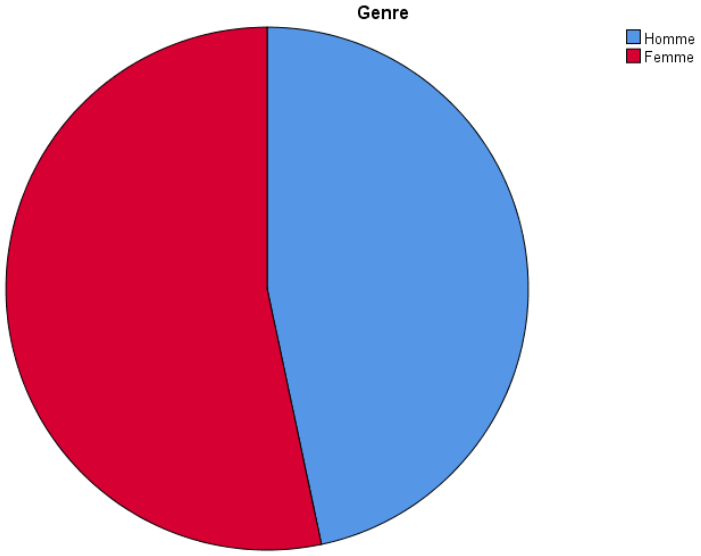


Figure 6 : représentation graphique de la répartition de l'échantillon selon le genre.

Source : Établi par nous-mêmes à partir de SPSS.

A partir du tableau 3 et la figure 8, qui représentent la répartition de l'échantillon selon le genre, on remarque une répartition équilibrée entre les sexes. Sur un total de 120 répondants, 53.3 % sont des femmes tandis que 46.7 % sont des hommes. Cette répartition équilibrée entre hommes et femmes est importante car elle permet d'obtenir des perspectives diverses et complémentaires sur la question de la gouvernance électronique et de la sécurité des données. Les expériences et les perceptions peuvent varier en fonction du

genre, et une représentation équilibrée permet de mieux comprendre ces différences et d'obtenir des résultats plus complets.

Question : Quel âge avez-vous ?

Tableau 4 : la répartition des interrogés selon l'âge.

Variable	Fréquence	%
Entre 20 et 29 ans	28	23.3
Entre 30 et 39 ans	25	20.8
Entre 40 et 49 ans	35	29.2
Entre 50 et 59 ans	29	24.2
60 ans et plus	3	2.5
Total	120	100.0

Source : Établi par nous-mêmes sur la base des résultats sur spss.

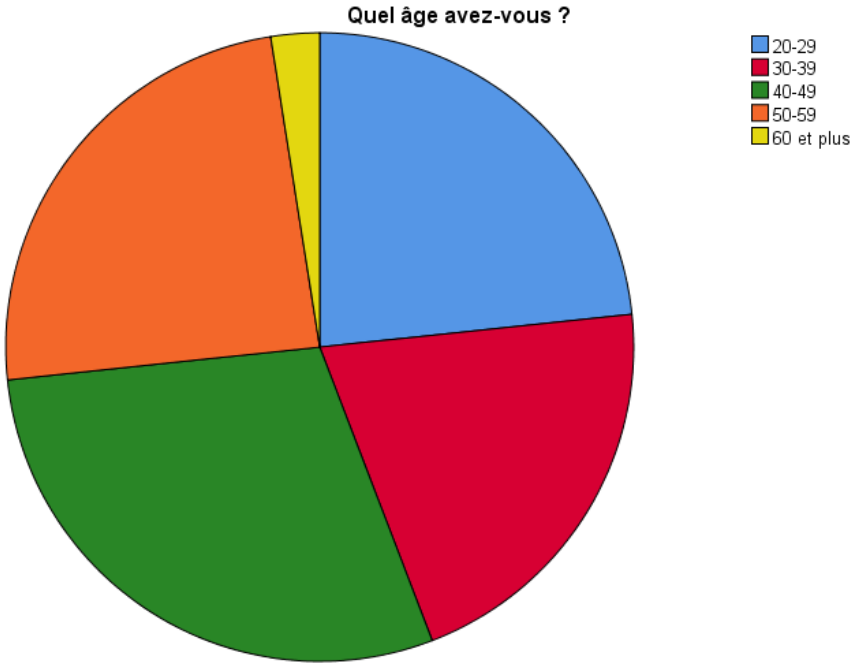


Figure 7 : Représentation graphique de la répartition de l'échantillon selon l'âge.

Source : Établi par nous-mêmes à partir de SPSS.

Le tableau 4 et la figure 9 représentent la répartition des répondants en fonction de leur âge. Ces données montrent une distribution diversifiée dans l'échantillon. La catégorie d'âge la plus représentée est celle des 40-49 ans (soit 29.2%), suivie de près par les 50-59 ans (soit 24.2%). Les personnes âgées de 20 à 29 ans et de 30 à 39 ans sont

également bien représentées (23.3%, 20.8%, respectivement), tandis que les personnes de 60 ans et plus sont moins nombreuses dans l'échantillon (soit 2.5% seulement). Cette répartition diversifiée selon l'âge est importante car elle permet d'obtenir des perspectives variées sur la question de la gouvernance électronique et de la sécurité des données. Les différentes catégories d'âge peuvent avoir des préoccupations et des expériences différentes en matière de sécurité des données, ce qui peut influencer la manière dont ils perçoivent les pratiques de gouvernance électronique au sein d'Algérie Télécom.

Question : Quelle est votre poste au sein d'Algérie Télécom ?

Tableau 5 : Répartition selon le poste au sein d'Algérie Télécom.

Variable	Fréquence	%
Agent de maîtrise	27	22.5
Cadre	73	60.8
Cadre supérieur	20	16.7
Total	120	100.0

Source : Établi par nous-mêmes sur la base des résultats sur spss.

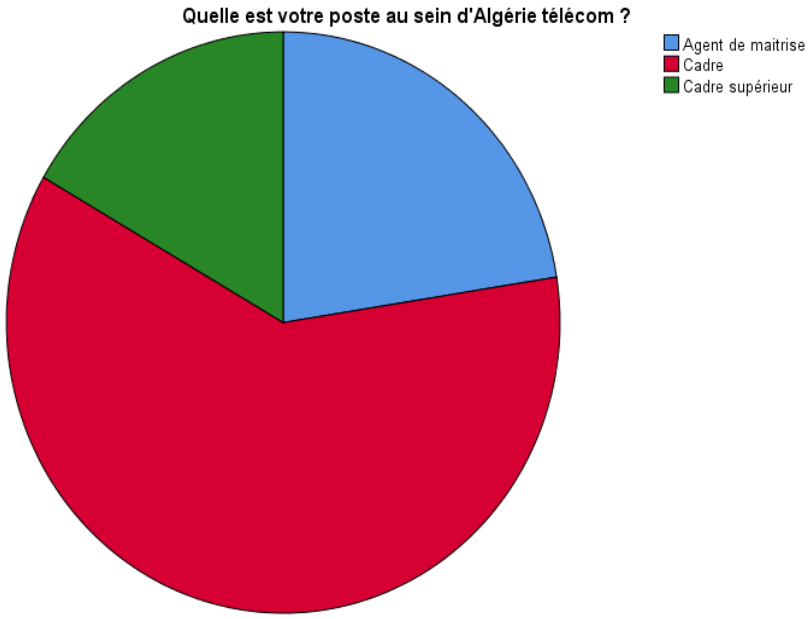


Figure 8 : Représentation graphique de la répartition selon le poste au sein d'Algérie télécom.

Source : Établi par nous-mêmes à partir de SPSS.

Le tableau 5 et la figure 10 représentent la répartition des répondants selon leur poste au sein d'Algérie Télécom. Cette répartition montre que la majorité des répondants sont des

cadres avec 60,8 %, suivis par les agents de maîtrise à 22,5 % et les cadres supérieurs à 16,7 %. Cette répartition diversifiée des postes au sein de l'entreprise est importante car elle permet d'obtenir des perspectives variées sur la gouvernance électronique et la sécurité des données. La grande majorité des cadres peut apporter une compréhension approfondie des politiques et des pratiques de gouvernance électronique mises en place, ainsi que de leur efficacité perçue. Les agents de maîtrise, quant à eux, peuvent offrir des perceptions précieuses sur la mise en œuvre pratique de ces politiques au niveau opérationnel. Enfin, les cadres supérieurs peuvent fournir une vision stratégique et des orientations sur les objectifs et les priorités en matière de gouvernance électronique.

Question : Depuis combien de temps travailler-vous chez Algérie Télécom ?

Tableau 6 : Répartition de l'échantillon selon l'expérience.

Variable	Fréquence	%
Moins de 5 ans	19	15.8
5-10 ans	36	30.0
11 a 15 ans	46	38.3
16 a 20 ans	14	11.7
Plus de 20 ans	5	4.2
Total	120	100.0

Source : Établi par nous-mêmes sur la base des résultats sur spss.

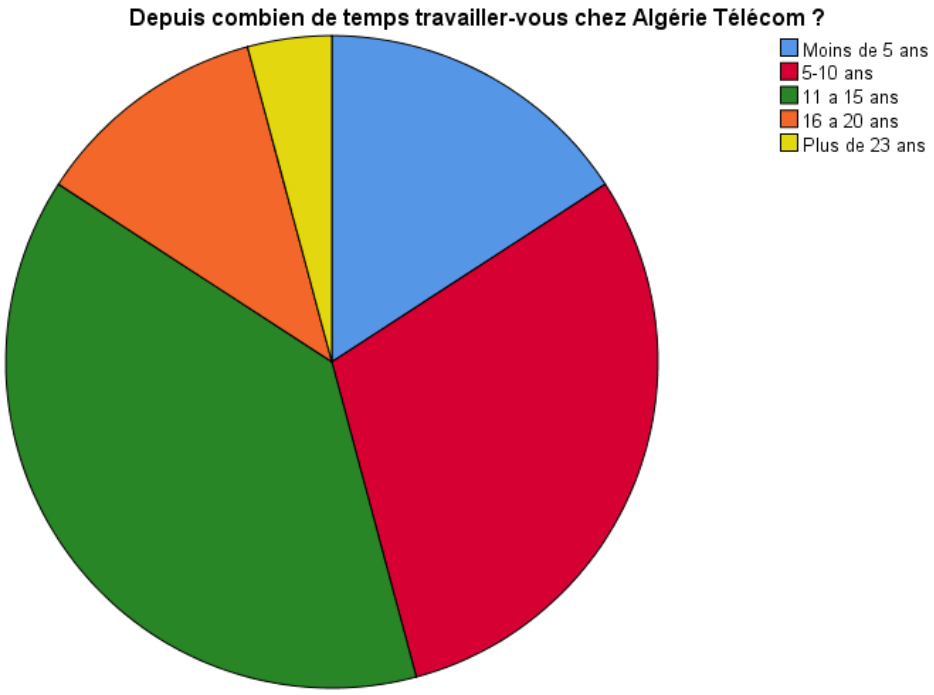


Figure 9 : représentation graphique de la répartition selon l'expérience.

Source : Établi par nous-mêmes à partir de SPSS.

Le tableau 6 et la figure 11 relatives à la répartition des répondants selon leur expérience de travail chez Algérie Télécom montrent une diversité significative, avec une forte proportion des répondants ayant entre 5 et 15 ans d'expérience (68.3 %) dans l'échantillon ce qui suggère une main-d'œuvre relativement stable et expérimentée au sein de l'entreprise. Les répondants ayant moins de 5 ans d'expérience (soit 15.8%) peuvent offrir des perspectives nouvelles et fraîches sur les pratiques de gouvernance électronique, tandis que ceux ayant plus de 15 ans d'expérience (11.7%) peuvent apporter une compréhension approfondie de l'évolution de ces pratiques au fil du temps. La proportion de répondants ayant plus de 20 ans d'expérience est relativement faible (4,2 %), ce qui peut limiter la représentativité de ce groupe dans l'échantillon. Cependant, ces répondants peuvent offrir des perspectives uniques en tant qu'employés ayant une longue expérience au sein de l'entreprise.

2. Connaissances générales sur la gouvernance électronique et la sécurité des données

Question : Etes-vous familier avec le concept de gouvernance électronique ?

Tableau 7 : Répartition de l'échantillon.

Variable	Fréquence	%
Oui	108	90.0
Non	12	10.0
Total	120	100.0

Source : Établi par nous-mêmes sur la base des résultats sur Spss.

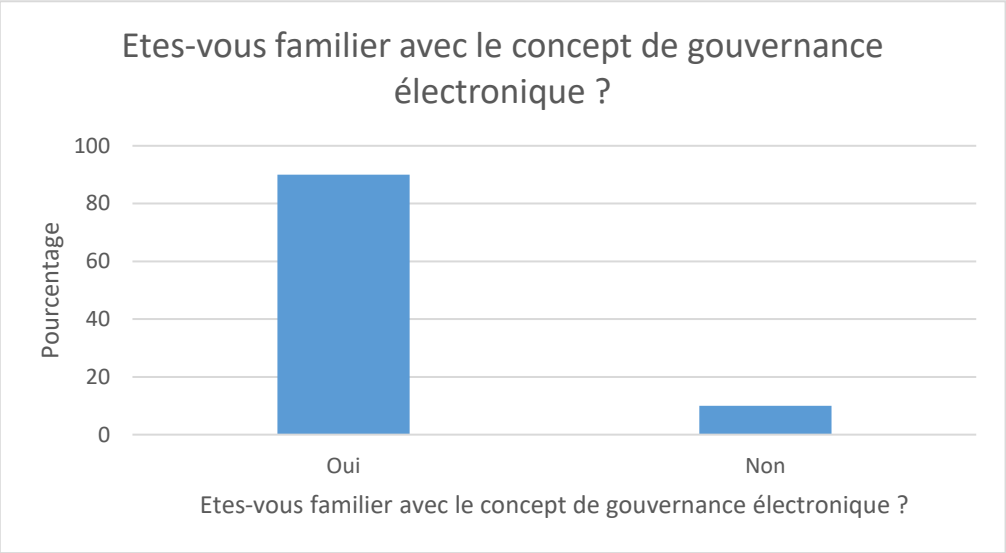


Figure 10 : représentation graphique de la répartition.

Source : Établi par nous-mêmes à partir de SPSS.

Le tableau 7 et la figure 12 indiquent que la majorité des répondants (90,0 %) sont familiers avec le concept de gouvernance électronique, tandis qu'une minorité (10,0 %) ils ne sont pas. Cette forte proportion de répondants familiers avec la gouvernance électronique suggère une certaine sensibilisation et compréhension de ce concept au sein de l'entreprise, ce qui peut être bénéfique pour la mise en œuvre de pratiques de gouvernance efficaces en matière de sécurité des données.

Question : Comment évaluez-vous votre niveau connaissance en matière de sécurité des données et de gouvernance électronique ?

Tableau 8 : Répartition de l'échantillon.

variable	Fréquence	%
Très faible	10	8.3
Faible	27	22.5
Neutre	46	38.3
Elevé	30	25.0
Très élevé	7	5.8
Total	120	100.0

Source : Etabli par nous-mêmes sur la base des résultats sur spss.

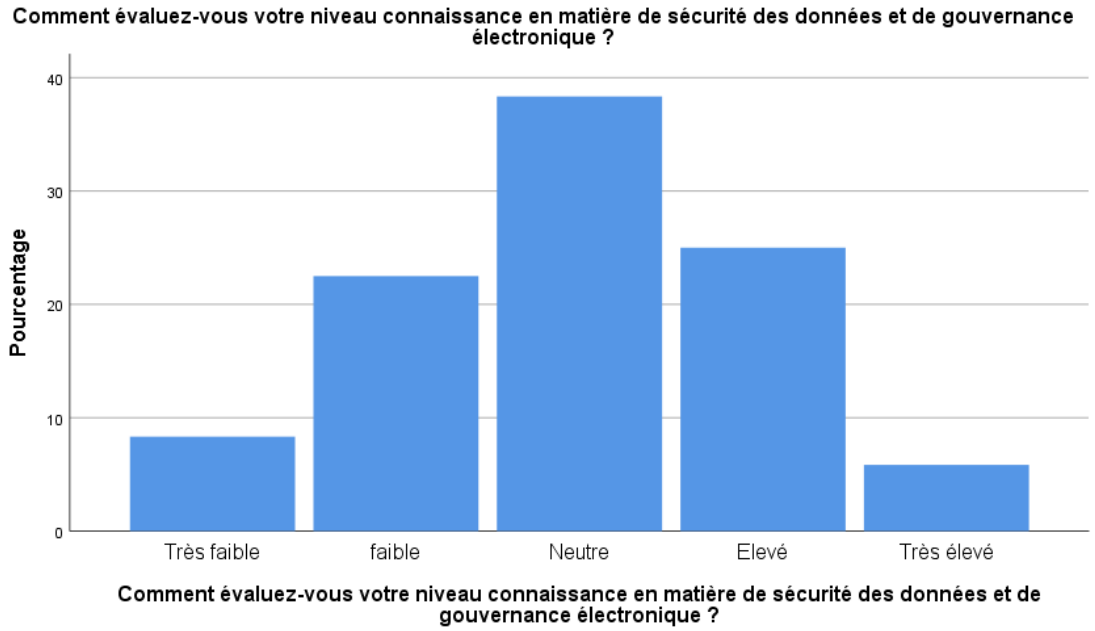


Figure 11 : représentation graphique de la répartition.

Source : Établi par nous-mêmes à partir de SPSS.

Le tableau 8 et la figure 13 montrent une distribution variée des évaluations du niveau de connaissance en matière de sécurité des données et de gouvernance électronique. La majorité des répondants (63,3 %) évaluent leur niveau de connaissance comme étant neutre (38.3%) ou supérieur (élevé soit 25%, très élevé soit 5.8%). Cette diversité des niveaux de connaissance en matière de sécurité des données et de gouvernance électronique peut influencer leur compréhension et leur interprétation des questions liées à ces domaines.

Question : Avez-vous reçu une formation sur la sécurité des données et la gouvernance électronique ?

Tableau 9 : Répartition de l'échantillon.

Variable	Fréquence	%
Oui	42	35.0
Non	78	65.0
Total	120	100.0

Source : Établi par nous-mêmes sur la base des résultats sur spss.

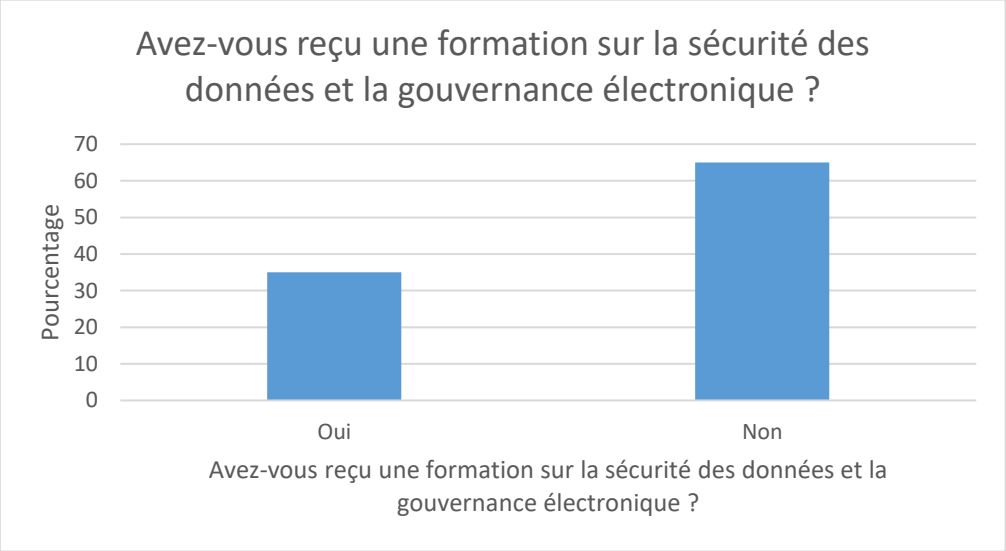


Figure 12 : représentation graphique de la répartition.

Source : Établi par nous-mêmes à partir de SPSS.

Le tableau 9 et la figure 14 montrent qu'une proportion significative (65,0 %) n'a pas reçu de formation dans ces domaines. Cette absence de formation met en lumière un besoin potentiel d'amélioration des initiatives de formation pour renforcer les connaissances et les compétences des employés dans ces domaines cruciaux. Cette lacune peut également souligner l'importance pour Algérie Télécom d'investir dans des programmes de formation pour sensibiliser et préparer ses employés à faire face aux défis croissants en matière de sécurité des données.

Question : Comment évaluez-vous la conformité d'Algérie Télécom aux réglementations en matière de protection des données ?

Tableau 10 : Répartition de l'échantillon.

Variable	Fréquence	%
Très mauvaise	4	3.3
Mauvaise	6	5.0
Neutre	39	32.5
Bonne	61	50.8
Excellente	10	8.3
Total	120	100.0

Source : Établi par nous-mêmes sur la base des résultats sur spss.

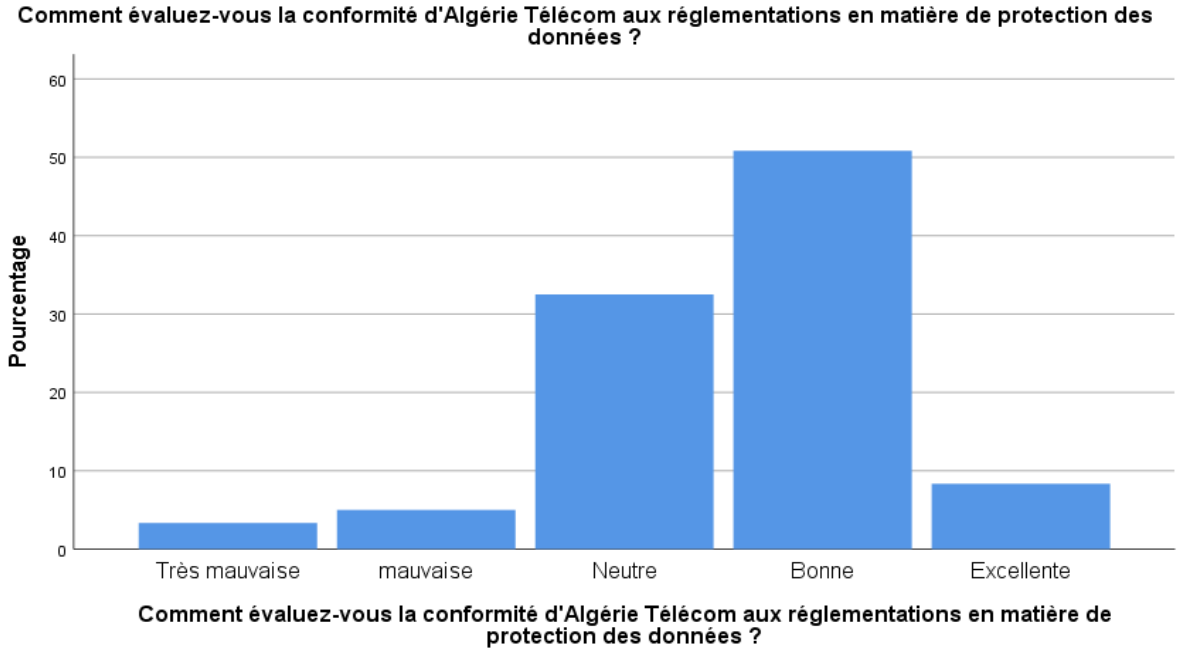


Figure 13 : Représentation graphique de la répartition.

Source : Établi par nous-mêmes à partir de SPSS.

Le tableau 10 et la figure 15 montrent que la majorité des répondants (59,1 %) évaluent la conformité comme étant bonne ou excellente, ce qui suggère une certaine confiance dans les pratiques de l'entreprise en matière de protection des données. Cependant, une minorité de répondants (8,3 %) considèrent la conformité comme étant très mauvaise ou mauvaise, ce qui indique qu'il existe des préoccupations ou des domaines à améliorer.

Cette perception positive de la conformité aux réglementations est le résultat d'efforts déployés par Algérie Télécom pour se conformer aux normes en matière de protection des données.

Question : Comment évaluez-vous la transparence d'Algérie Telecom en ce qui concerne la gestion et la protection des données personnelles ?

Tableau 11 : Répartition de l'échantillon.

Variable	Fréquence	%
Pas du tout transparente	5	4.2
Peu transparente	12	10.0
Neutre	26	21.7
Transparente	64	53.3
Très transparente	13	10.8
Total	120	100.0

Source : Établi par nous-mêmes sur la base des résultats sur spss.

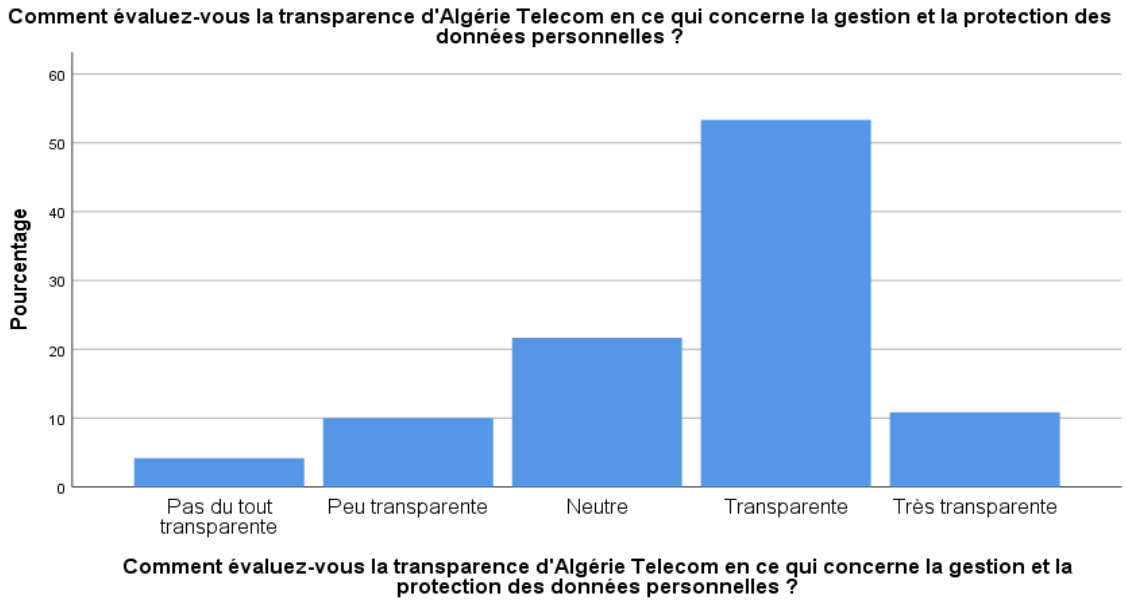


Figure 14 : représentation graphique de la répartition.

Source : Établi par nous-mêmes à partir de SPSS.

Le tableau 11 et la figure 16 indiquent que la majorité de répondants (64,1 %) évaluent la transparence d'Algérie Télécom en ce qui concerne la gestion et la protection des données personnelles comme étant transparente (soit 53.3) ou très transparente (soit 10.8%), ce qui suggère une confiance relative dans les pratiques de l'entreprise en matière de gestion et de protection des données personnelles. Cette perception positive est le résultat d'une communication efficace de la part d'Algérie Télécom sur ses pratiques et ses engagements

en matière de protection des données. Cependant, une minorité de répondants (14,2 %) considèrent la transparence comme étant pas du tout transparente ou peu transparente. Cela indique qu'il existe des préoccupations ou des perceptions négatives quant à la transparence de l'entreprise en matière de gestion des données personnelles. Ces évaluations moins positives soulignent la nécessité pour Algérie Télécom d'améliorer sa communication et sa transparence dans ce domaine afin de renforcer la confiance des employés dans ses pratiques de gestion des données personnelles.

Question : Comment décririez-vous la culture de la sécurité des données au sein de l'entreprise ?

Tableau 12 : Répartition de l'échantillon.

Variable	Fréquence	%
Très Faible	7	5.8
Faible	8	6.7
Neutre	34	28.3
Forte	55	45.8
Très forte	16	13.3
Total	120	100.0

Source : Établi par nous-mêmes sur la base des résultats sur spss.

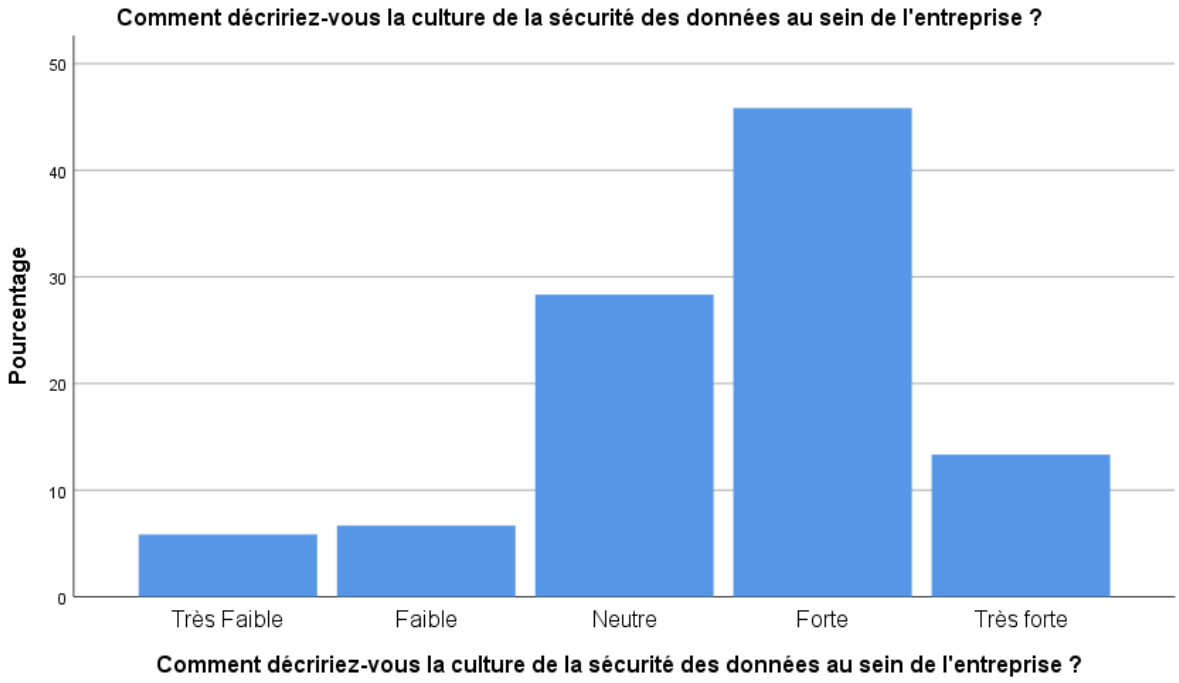


Figure 15 : Représentation graphique de la répartition.

Source : Établi par nous-mêmes à partir de SPSS.

Le tableau 12 et la figure 17 montrent une perception majoritairement positive de la culture de la sécurité des données au sein d'Algérie Télécom. La majorité des répondants (59,1 %) évaluent la culture comme étant forte (soit 45.8%) ou très forte (soit 13.3%), ce qui montre une sensibilisation et une importance accordée à la sécurité des données au sein de l'entreprise. Cette perception positive est le résultat d'efforts déployés par l'entreprise pour promouvoir une culture de sécurité des données, tels que des formations, des politiques claires et une sensibilisation des employés. Cependant, une minorité (12,5 %) la considère comme très faible ou faible. Cela indique qu'il existe des domaines où des améliorations peuvent être apportées pour renforcer la culture de la sécurité des données au sein d'Algérie Télécom. Ces résultats soulignent l'importance de poursuivre les efforts visant à sensibiliser et à impliquer les employés dans la protection des données.

3. Mesures de sécurité et pratiques de gouvernance électronique

Question : Êtes-vous satisfait(e) des mesures de gouvernance électronique mises en place par Algérie Telecom ?

Tableau 13 : Répartition de l'échantillon.

Variable	Fréquence	%
Pas du tout satisfait(e)	6	5.0
Peu satisfait(e)	25	20.8
Neutre	29	24.2
Satisfait(e)	47	39.2
Très satisfait(e)	13	10.8
Total	120	100.0

Source : Établi par nous-mêmes sur la base des résultats sur spss.

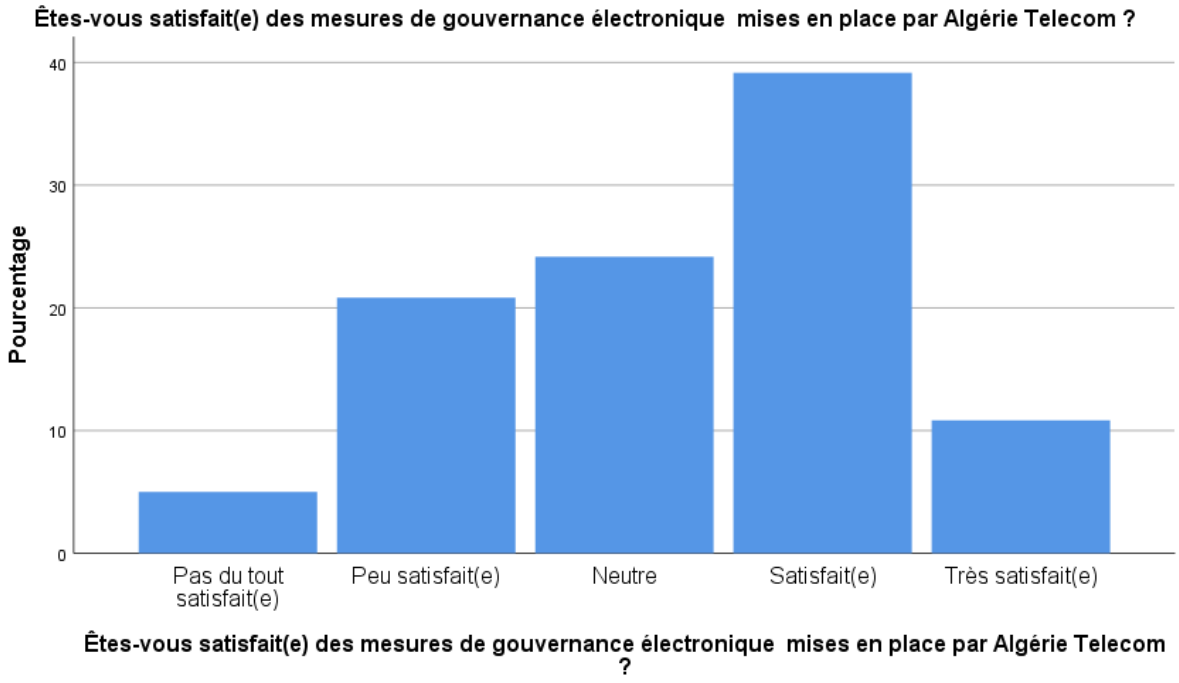


Figure 16 : représentation graphique de la répartition.

Source : Établi par nous-mêmes à partir de SPSS.

Le tableau 13 et la figure 18 montrent une satisfaction générale envers les mesures de gouvernance électronique mises en place par Algérie Telecom. Une majorité des

répondants (49,2 %) se disent satisfaits ou très satisfaits, ce qui montre une perception positive des efforts de l'entreprise dans ce domaine. Cette satisfaction est le résultat d'une gouvernance électronique efficace, de processus de surveillance réguliers et de la capacité à détecter et prévenir les violations de données et les accès non autorisés aux informations sensibles des citoyens. Cependant, une minorité de répondants (25,8 %) se dit peu satisfaite ou pas du tout satisfaite. Cela indique qu'il existe des domaines où des améliorations peuvent être apportées pour renforcer la satisfaction des employés à l'égard des mesures de gouvernance électronique. Ces résultats soulignent l'importance pour Algérie Telecom de continuer à évaluer et à améliorer ses pratiques de gouvernance électronique pour répondre aux attentes et aux besoins de ses employés.

Question : À quel point faites-vous confiance aux systèmes de sécurité des données mis en place par l'entreprise ?

Tableau 14 : Répartition de l'échantillon.

Variable	Fréquence	%
Pas du tout confiant(e)	6	5.0
Peu confiant(e)	12	10.0
Neutre	36	30.0
Confiant(e)	52	43.3
Très confiant(e)	14	11.7
Total	120	100.0

Source : Établi par nous-mêmes à partir de SPSS.

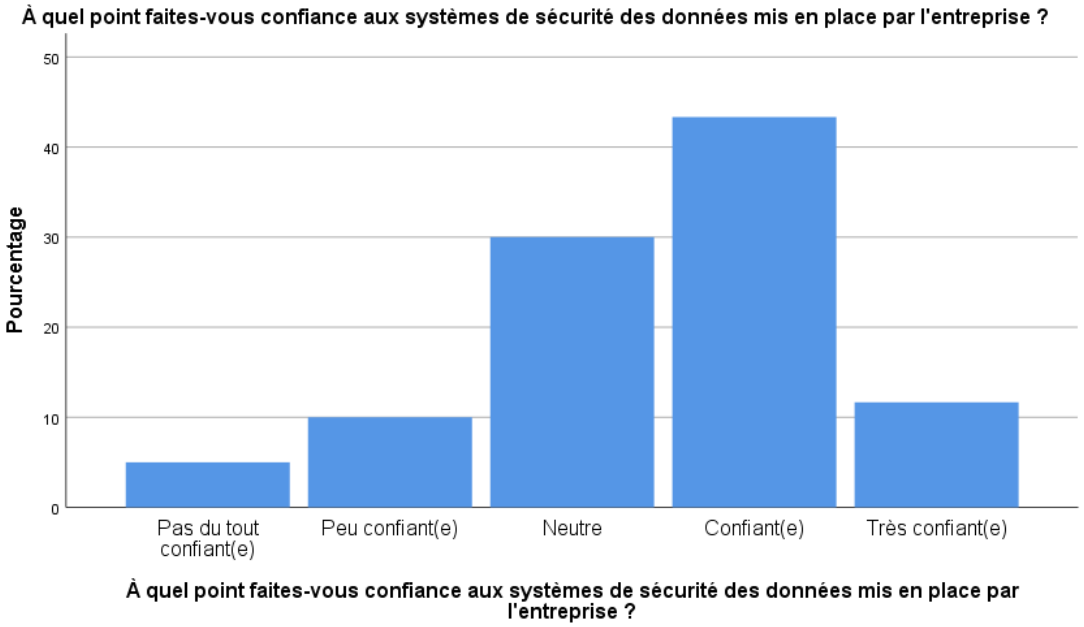


Figure 17 : représentation graphique de la répartition.

Source : Établi par nous-mêmes à partir de l'EXCEL et SPSS.

Le tableau 14 et la figure 19 montrent un niveau de confiance généralement élevé dans les systèmes de sécurité des données mis en place par Algérie Telecom. Une majorité de répondants (54,2 %) se disent confiants ou très confiants dans les systèmes de sécurité des données, ce qui indique une perception positive de l'efficacité de ces systèmes. Cette confiance est le résultat de mesures de sécurité robustes mises en place par l'entreprise, ainsi que d'une communication efficace sur les pratiques de sécurité des données. Cependant, une minorité de répondants (15,0 %) se dit peu confiante ou pas du tout confiante. Cela indique qu'il existe des préoccupations ou des perceptions négatives quant à l'efficacité des systèmes de sécurité des données.

Question : Pensez-vous que la gouvernance électronique peut contribuer à réduire les risques liés à la sécurité des données ?

Tableau 15 : Répartition de l'échantillon.

Variable	Fréquence	%
Oui	112	93.3
Non	8	6.7
Total	120	100.0

Source : Établi par nous-mêmes sur la base des résultats sur spss.

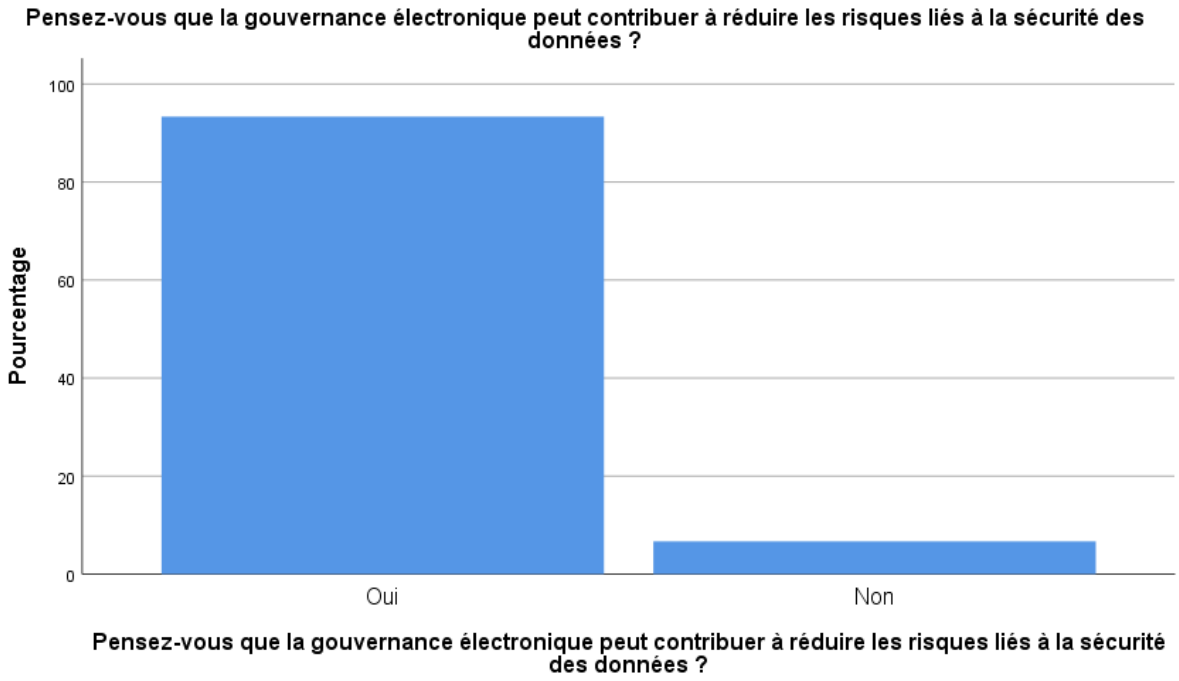


Figure 18 : représentation graphique de la répartition.

Source : Établi par nous-mêmes à partir de SPSS.

Le tableau 15 et la figure 20 montrent une perception très positive de la contribution de la gouvernance électronique à la réduction des risques liés à la sécurité des données. Une grande majorité des répondants (93,3 %) estiment que la gouvernance électronique peut contribuer à réduire ces risques. Cette perception positive montre une reconnaissance de l'importance de la gouvernance électronique dans la protection des données et souligne l'importance accordée à la mise en place de mesures de gouvernance efficaces pour garantir la sécurité des données. Ces résultats indiquent également une sensibilisation accrue des répondants aux enjeux de sécurité des données et à l'impact positif que peut avoir une gouvernance électronique efficace dans ce domaine.

Question : Selon vous, quels sont les principaux défis liés à la gouvernance électronique pour garantir la sécurité des données ?

Tableau 16 : Répartition de l'échantillon.

Variable	Oui	%	Non	%
Protection des données personnelles	45	37.5 %	75	62.5 %
Sécurité des infrastructures	64	53.3 %	56	46.7 %
Sensibilisation et formation	64	53.3 %	56	46.7 %
Manque de ressource	18	15.0 %	102	85.0 %
Complexité des systèmes	66	55.0 %	54	45.0 %

Source : Établi par nous-mêmes sur la base des résultats sur spss.

La répartition des répondants selon leurs perceptions des principaux défis liés à la gouvernance électronique pour garantir la sécurité des données montre une diversité d'opinions :

La protection des données personnelles est identifiée comme un défi majeur par 37,5 % des répondants, ce qui souligne l'importance accordée à la confidentialité des données.

La sécurité des infrastructures est également considérée comme un défi significatif par plus de la moitié des répondants (53,3 %), ce qui met en lumière l'importance des mesures de sécurité techniques pour protéger les données.

La sensibilisation et la formation sont également identifiées comme des défis importants par plus de la moitié des répondants (53,3 %). Cela souligne l'importance d'éduquer et de former le personnel sur les bonnes pratiques en matière de sécurité des données pour réduire les risques.

Le manque de ressources est un défi moins fréquemment mentionné, mais tout de même pertinent, selon 15,0 % des répondants. Enfin, **la complexité des systèmes** est identifiée comme un défi majeur par plus de la moitié des répondants (55,0 %), soulignant la nécessité de simplifier les systèmes pour améliorer la sécurité des données.

Ces résultats soulignent la complexité et la diversité des défis auxquels les organisations sont confrontées en matière de gouvernance électronique pour garantir la sécurité des données. Ils mettent en évidence la nécessité d'une approche intégrée de la gouvernance électronique, qui prend en compte non seulement les aspects techniques, mais aussi les

aspects humains, organisationnels et financiers pour assurer une protection efficace des données.

Question : Dans quelle mesure considérez-vous que la gouvernance électronique des données soit importante pour assurer la sécurité des données au sein de l'entreprise ?

Tableau 17 : Répartition de l'échantillon.

Variable	Fréquence	%
Pas du tout important	2	1.7
Peu important	9	7.5
Neutre	29	24.2
Important	35	29.2
Très important	45	37.5
Total	120	100.0

Source : Établi par nous-mêmes sur la base des résultats sur spss.

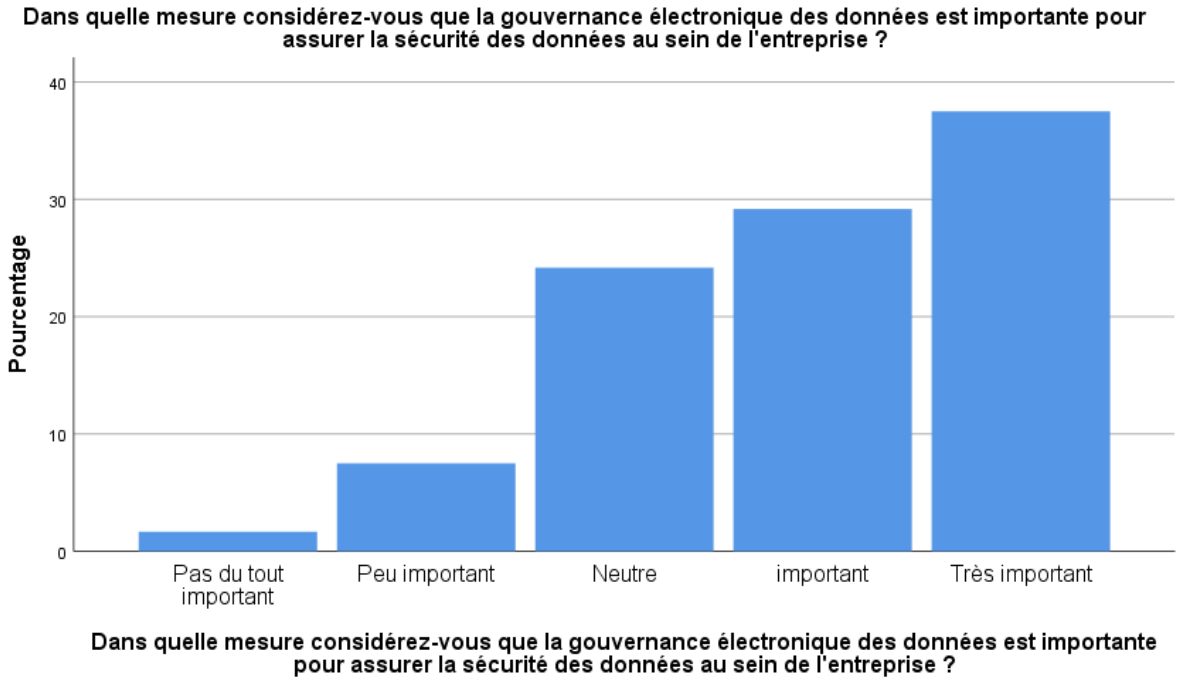


Figure 19 : représentation graphique de la répartition.

Source : Établi par nous-mêmes à partir de SPSS.

Le tableau 17 et la figure 21 qui indiquent la répartition des répondants selon leur perception de l'importance de la gouvernance électronique des données pour assurer la

sécurité des données au sein de l'entreprise, montrent une reconnaissance générale de son importance. Une majorité significative de répondants (66,7 %) considèrent la gouvernance électronique des données comme importante ou très importante pour assurer la sécurité des données. Cela indique une prise de conscience de l'importance d'une gouvernance efficace pour garantir la sécurité des données au sein de l'entreprise.

Question : À votre avis, quelles pourraient être les conséquences d'une mauvaise gouvernance électronique sur la réputation d'Algérie Télécom ?

Tableau 18 : Répartition de l'échantillon.

Variable	Oui	%	Non	%
Perte de clients	84	70.0 %	36	30.0 %
Pertes financières	74	61.7 %	46	38.3 %
Cyberattaques	76	63.3 %	44	36.7 %
Violations de la vie privée	55	45.8 %	65	54.2 %
Pannes et interruptions de service	58	48.3 %	62	51.7 %

Source : Établi par nous-mêmes sur la base des résultats sur spss.

La répartition des répondants selon leurs perceptions des conséquences d'une mauvaise gouvernance électronique sur la réputation d'Algérie Télécom met en évidence plusieurs préoccupations importantes.

Une majorité significative de répondants sont préoccupés par la possibilité d'une perte de clients (70,0 %), de pertes financières (61,7 %) et de cyberattaques (63,3 %) en cas de mauvaise gouvernance électronique. Ces résultats soulignent l'importance pour Algérie Télécom de mettre en place une gouvernance électronique solide pour protéger sa réputation et ses activités commerciales. Les répondants sont également sensibles aux risques potentiels pour la vie privée des clients (45,8 %) et aux pannes et interruptions de service (48,3 %) qui pourraient résulter d'une mauvaise gouvernance électronique. Ces résultats mettent en lumière l'importance d'une gouvernance électronique efficace pour maintenir la confiance des clients et assurer le bon fonctionnement des services de l'entreprise.

Question : Trouviez-vous que le nombre d'incidents de sécurité a diminué grâce à la gouvernance électronique ?

Tableau 19 : Répartition de l'échantillon.

Variable	Fréquence	%
Oui	96	80.0
Non	24	20.0
Total	120	100.0

Source : Établi par nous-mêmes sur la base des résultats sur spss.

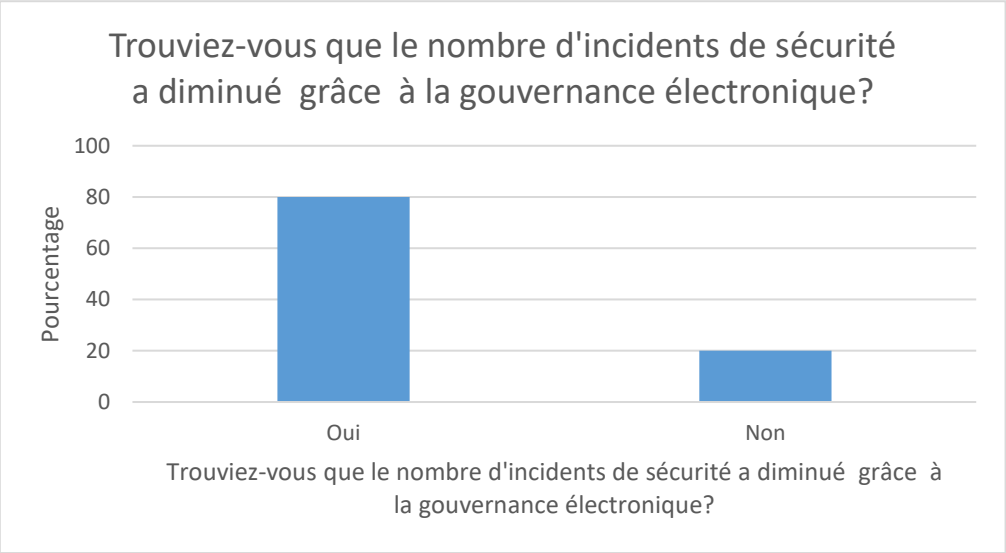


Figure 20 : représentation graphique de la répartition.

Source : Établi par nous-mêmes à partir de SPSS.

Le tableau 19 et la figure 22 montrent la répartition des répondants selon leur perception de l'impact de la gouvernance électronique sur la diminution du nombre d'incidents de sécurité. Ces résultats montrent une tendance positive. La grande majorité des répondants (80,0 %) estiment que le nombre d'incidents de sécurité a diminué grâce à la gouvernance électronique. Cela montre que la gouvernance électronique mise en place par Algérie Télécom a eu un impact positif sur la sécurité des données et la réduction des incidents de sécurité.

Question : Pensez-vous que les clients d'Algérie Télécom sont conscients des efforts de l'entreprise en matière de gouvernance électronique et de sécurité des données ?

Tableau 20 : Répartition de l'échantillon.

Variable	Fréquence	%
Oui	46	38.3
Non	74	61.7
Total	120	100.0

Source : Établi par nous-mêmes sur la base des résultats sur spss.

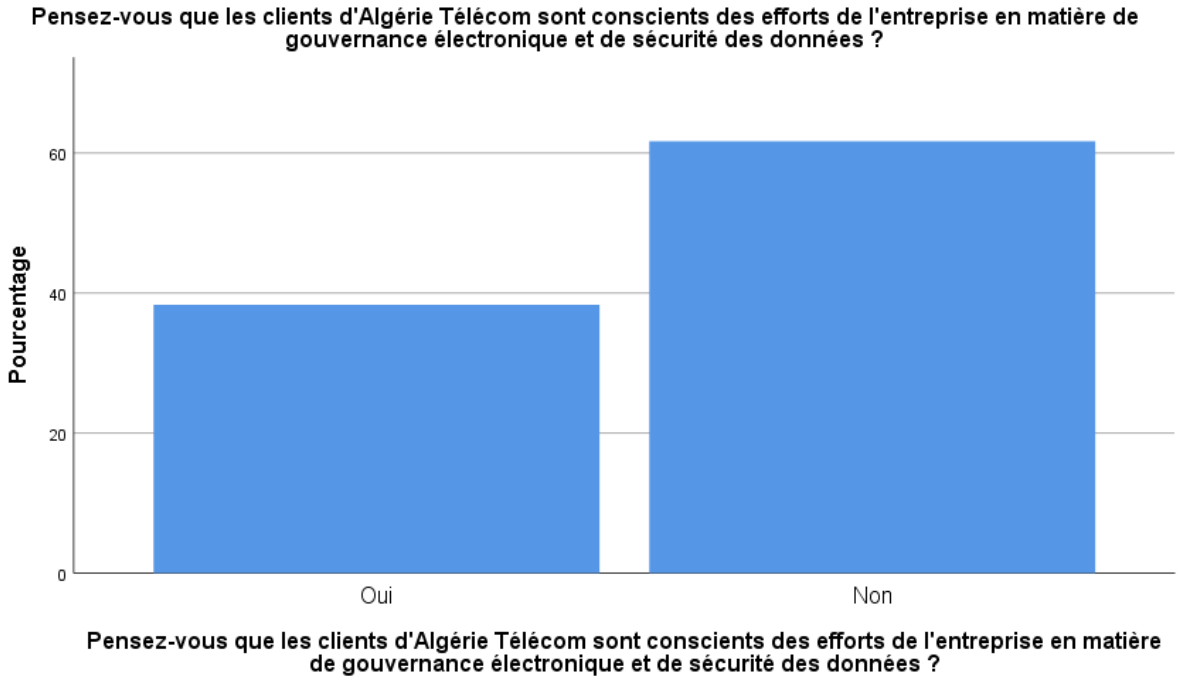


Figure 21 : représentation graphique de la répartition.

Source : Établi par nous-mêmes à partir de SPSS.

Le tableau 20 et la figure 23 montrent qu'majorité significative de répondants (61,7 %) estime que les clients d'Algérie Télécom ne sont pas conscients des efforts de l'entreprise en matière de gouvernance électronique et de sécurité des données. Cela soulève des questions sur la communication et la sensibilisation des clients aux initiatives et aux mesures prises par l'entreprise pour garantir la sécurité des données. Tandis que seulement 38,3 % des répondants pensent que les clients sont conscients des efforts de l'entreprise. Cela suggère qu'il peut y avoir un besoin accru de communication et de transparence pour informer efficacement ses clients de ses actions en matière de gouvernance électronique et de sécurité des données.

Question : Avez-vous des suggestions ou des recommandations pour améliorer la sécurité des données et la gouvernance électronique chez Algérie Télécom ? (Question ouverte)

L'analyse de contenu des réponses à cette question indique plusieurs thèmes clés :

1. Recrutement et formation du personnel : Plusieurs répondants suggèrent le recrutement de personnel qualifié en matière de gouvernance électronique ainsi que la sensibilisation et la formation continue des employés pour renforcer la sécurité des données.

2. Renforcement des systèmes de sécurité : Des recommandations incluent le renforcement des systèmes de sécurité, la mise à jour régulière des logiciels, la vigilance face aux emails et liens suspects, ainsi que la mise en place de politiques claires de sécurité des données.

3. Technologies et infrastructures : Certains répondants recommandent d'investir dans des technologies de pointe, de mettre en place des infrastructures solides, des systèmes de surveillance et de détection des intrusions.

4. Gestion des identités et des accès : La mise en place d'une gestion efficace des identités et des accès est également suggérée pour renforcer la sécurité des données.

5. Politiques et procédures : Il est recommandé de mettre en œuvre des politiques de sécurité des données claires et strictes, définissant les responsabilités, les procédures et les mesures de sécurité à suivre par le personnel.

En résumé, les suggestions et recommandations des répondants mettent en lumière l'importance du recrutement et de la formation du personnel, du renforcement des systèmes de sécurité, de l'investissement dans les technologies, de la mise en place de politiques claires et de la sensibilisation continue pour améliorer la sécurité des données et la gouvernance électronique chez Algérie Télécom.

4. La vérification des hypothèses

Tests et discussion des hypothèses de l'étude :

Pour prouver les hypothèses de l'étude et identifier la nature de la relation entre l’innovation frugale et le développement durable, l’analyse des hypothèses sera basée sur le coefficient de corrélation de Pearson et une analyse de régression simple pour découvrir l'existence de la corrélation entre les variables, et le coefficient de détermination r2 pour expliquer dans quelle mesure la variable indépendante contribue à l'interprétation de la variable dépendante par les éléments suivants :

Test de la première hypothèse

H0 : L'implémentation de la gouvernance électronique ne réduit pas de manière significative les menaces contre la sécurité des données chez Algérie Télécom.

H1 : L'implémentation de la gouvernance électronique réduit de manière significative les menaces contre la sécurité des données chez Algérie Télécom.

Résultats de la régression linéaire simple

Tableau 21 : Récapitulatif des modèles.

Modèle	R	R-deux	R-deux ajusté	Erreur standard de l'estimation
1	,025[a]	,001	-,008	,22494

Source : Élaboré par nous- même à partir des données du logiciel SPSS (V.25).

- Les coefficients (R) de corrélation et (R^2) de détermination sont très faible, ce qui signifie que le modèle de régression linéaire simple ne parvient pas à expliquer de manière significative la variation de la variable dépendante (réduction des menaces contre la sécurité des données) en fonction de l'implémentation de la gouvernance électronique.

Tableau 22 : ANOVA a.

Modèle		Somme des carrés	Ddl	Carré moyen	F	Sig.
1	Régression	,004	1	,004	,071	,790[b]
	de Student	5,970	118	,051		
	Total	5,974	119			

Source : Élaboré par nous- même à partir des données du logiciel SPSS (V.25).

- L'analyse de variance (ANOVA) montre que le modèle de régression n'est pas statistiquement significatif, avec un F de 0.071 et une valeur p de 0.790> 0.05. Cela signifie qu'il n'y a pas suffisamment de preuves pour rejeter l'hypothèse nulle selon laquelle l'implémentation de la gouvernance électronique ne réduit pas de manière significative les menaces contre la sécurité des données.

Tableau 23 : Coefficients a.

Modèle		Coefficients non standardisés		Coefficients standardisés	t	Sig.
		B	Erreur standard	Bêta		
1	(Constante)	,927	,090		10,282	,000
	L'implémentation de la gouvernance électronique	,022	,082	,025	,267	,790

Source : Élaboré par nous- même à partir des données du logiciel SPSS (V.25).

-Le coefficient B pour l'implémentation de la gouvernance électronique est de 0.022 avec une valeur p de 0.790, ce qui indique qu'il n'est pas statistiquement significatif. Cela confirme que l'implémentation de la gouvernance électronique n'a pas un effet significatif sur la réduction des menaces contre la sécurité des données.

En conclusion, les résultats de l'analyse de régression linéaire simple ne soutiennent pas l'hypothèse alternative selon laquelle l'implémentation de la gouvernance électronique réduit de manière significative les menaces contre la sécurité des données chez Algérie Télécom. Au contraire, les résultats suggèrent qu'il n'y a pas de lien significatif entre ces deux variables.

Test de la deuxième hypothèse : Bien que censée renforcer la protection des données, l'implémentation de la gouvernance électronique risque de ne pas réduire substantiellement les menaces contre la sécurité des données.

Hypothèse 0 : il n'existe pas une relation positive statistiquement significative entre les deux variables.

Hypothèse 1 : il existe une relation positive statistiquement significative entre les deux variables.

Résultats de la régression linéaire simple

Tableau 24 : Récapitulatif des modèles.

Modèle	R	R-deux	R-deux ajusté	Erreur standard de l'estimation
1	,644[a]	,415	,410	,63841

Source : Élaboré par nous- même à partir des données du logiciel SPSS (V.25).

Les résultats de la régression linéaire simple montrent une relation positive et significative entre une meilleure connaissance et une formation adéquate en matière de gouvernance électronique et de sécurité des données, et l'amélioration de la culture de sécurité ainsi que la réduction des risques liés aux données.

Le coefficient de corrélation (R) est de 0,644, indiquant une relation modérément forte entre les variables. Le coefficient de détermination (R^2) de 0,415 suggère que 41,5 % de la variance de la culture de sécurité peut être expliquée par la connaissance et la formation en gouvernance électronique et sécurité des données.

Tableau 25 : ANOVA a.

Modèle		Somme des carrés	ddl	Carré moyen	F	Sig.
1	Régression	34,084	1	34,084	83,628	,000[b]
	de Student	48,093	118	,408		
	Total	82,177	119			

Source : Élaboré par nous- même à partir des données du logiciel SPSS (V.25).

L'analyse de la variance (ANOVA) indique que le modèle de régression est significatif ($F(1, 118) = 83,628$, $p < 0,001$), ce qui suggère que la relation entre les variables est statistiquement significative.

Tableau 26 : Coefficients a.

Modèle		Coefficients non standardisés		Coefficients standardisés	t	Sig.
		B	Erreur standard	Bêta		
1	(Constante)	,288	,349		,825	,411
	Vindp	1,357	,148	,644	9,145	,000

Source : Élaboré par nous- même à partir des données du logiciel SPSS (V.25).

Le coefficient de la variable indépendante (Bêta) est de 0,644, ce qui signifie qu'une augmentation d'une unité dans la connaissance et la formation en gouvernance électronique et sécurité des données est associée à une augmentation de 0,644 unité dans l'amélioration de la culture de sécurité.

En conclusion, les résultats soutiennent l'hypothèse alternative (H1) selon laquelle une meilleure connaissance et une formation adéquate en matière de gouvernance électronique et de sécurité des données contribuent à améliorer la culture de sécurité et à réduire les risques liés aux données, renforçant ainsi la confiance des clients et des employés dans la protection de leurs données personnelles.

Section 2 : Discussion des résultats

L'étude réalisée auprès des employés d'Algérie Télécom apporte un éclairage important sur l'impact de la gouvernance électronique sur la sécurité des données au sein de l'entreprise. Les résultats obtenus rejoignent et renforcent plusieurs conclusions issues de la littérature existante, tout en mettant en lumière des défis et des opportunités spécifiques à ce contexte organisationnel.

Tout d'abord, les données recueillies indiquent que la majorité des répondants sont familiers avec le concept de gouvernance électronique, ce qui suggère une sensibilisation adéquate aux enjeux liés à ce domaine. Cette observation est conforme aux recommandations formulées par (Ullah, F.; Sepasgozar, S. M.; Wang, C., 2019), qui soulignent l'importance de la sensibilisation des citoyens aux bénéfices de l'e-gouvernance pour favoriser son adoption réussie. Cependant, l'étude révèle également des niveaux de connaissances hétérogènes en matière de sécurité des données et de gouvernance électronique parmi les employés. Cette disparité met en évidence la nécessité d'améliorer les initiatives de formation, un aspect également souligné par (Aloufi, A. A.; Vasarhelyi, M. A., 2022) comme étant crucial pour renforcer la confiance des citoyens envers l'e-gouvernement.

En ce qui concerne la conformité aux réglementations sur la protection des données, la perception globalement positive des répondants reflète les efforts déployés par Algérie Télécom pour se conformer aux normes en vigueur. Cette observation est en phase avec les conclusions de l'étude menée par (Tomo, A.; Todisco, M.; Ruggieri, M.; Vinci, M. B., 2021), qui soulignent l'importance de la gouvernance des données pour assurer la conformité réglementaire. Néanmoins, les préoccupations exprimées par une minorité de répondants mettent en évidence des domaines spécifiques nécessitant des améliorations, notamment en matière de transparence sur la gestion des données personnelles. Ce constat rejoint les conclusions de (Aloufi, A. A.; Vasarhelyi, M. A., 2022), qui insistent sur la nécessité de renforcer la transparence pour accroître la confiance des citoyens.

La perception d'une culture de sécurité des données forte au sein d'Algérie Télécom témoigne des efforts déployés par l'entreprise pour promouvoir cette culture, tels que la formation, la sensibilisation et la mise en place de politiques claires. Cette observation positive est cohérente avec les recommandations formulées dans la littérature, notamment celles de (Zissis, D.; Lekkas, D., 2012), qui soulignent l'importance d'une architecture cloud sécurisée intégrant des contrôles de sécurité à tous les niveaux.

Malgré ces aspects positifs, l'étude met en lumière plusieurs défis auxquels Algérie Télécom doit faire face, notamment la complexité des systèmes, la sécurité des infrastructures, la sensibilisation et la formation, la protection des données personnelles, ainsi que le manque de ressources. Ces défis sont cohérents avec ceux identifiés dans la littérature, tels que les préoccupations liées à la sécurité des infrastructures, à la sensibilisation et à la formation, soulignée par (Zissis, D.; Lekkas, D., 2012), dans le contexte du cloud computing.

Néanmoins, les résultats de l'étude confirment unanimement la contribution significative de la gouvernance électronique à la réduction des risques liés à la sécurité des données. Cette reconnaissance rejoint les conclusions de (Hashim, Muhammad; Mahfooz, Bakhtawar; Ibrahim, Kainat, 2023), qui mettent en évidence l'importance de la gouvernance en matière de sécurité des données dans le secteur bancaire.

En résumé, cette étude apporte une contribution substantielle à la compréhension de l'impact de la gouvernance électronique sur la sécurité des données au sein d'une organisation spécifique, tout en renforçant et en étayant les conclusions issues de la littérature existante. Bien que des défis subsistent, les résultats soulignent l'importance cruciale d'une approche globale et continue de la gouvernance électronique, intégrant des aspects tels que la formation, la transparence, la conformité réglementaire et la gestion des ressources, pour assurer une protection adéquate des données et maintenir la confiance des parties prenantes.

CONCLUSION

Notre travail de recherche a pour objectif principal d’étudier l'impact de la gouvernance électronique sur la sécurité des données chez les employés d'Algérie Télécom. la question de recherche se voit combiner deux variables différentes, il s'agit de la gouvernance électronique et la sécurité des données.

Pour répondre à cette problématique, l'étude suit une approche d'analyse post positiviste. Bien que les résultats obtenus ne soient pas généralisables, ils permettent de vérifier les hypothèses formulées.

Pour ce faire, le modèle d'analyse établit une connexion entre la réflexion théorique sur la gouvernance électronique et son impact aux niveaux macro et micro, ainsi que le modèle de sécurité des données.

À partir de l'analyse théorique, il est pertinent de noter que la littérature sur la gouvernance électronique chez Algérie Télécom est fortement orientée vers l'amélioration de la sécurité des données. Les études sur les mécanismes de protection en Algérie, et en particulier les initiatives de cybersécurité, se concentrent principalement sur des méthodes de surveillance proactive.

À travers une méthodologie rigoureuse et une étude quantitative, les résultats ont permis de mettre en lumière des aspects clés liés à la sensibilisation des employés, la conformité, la culture de sécurité, les défis et l'importance de la gouvernance électronique. Afin de vérifier la validité de nos deux hypothèses, retenus de notre revue de littérature, nous avons opéré une analyse inférentielle à travers des régressions linéaires simples qui est censé d’étudier l’influence d’une variable indépendante ou plusieurs sur une seule variable dépendante ce qui le cas de notre recherche.

Les résultats soutiennent l'hypothèse alternative (H1) selon laquelle une meilleure connaissance et une formation adéquate en matière de gouvernance électronique et de sécurité des données contribuent à améliorer la culture de sécurité et à réduire les risques liés aux données, renforçant ainsi la confiance des clients et des employés dans la protection de leurs données personnelles.

Apport théorique

En s'appuyant sur une revue de littérature solide et une méthodologie d'analyse quantitative, cette étude contribue à la compréhension de l'importance de la gouvernance électronique dans la protection des données. Les résultats mettent en évidence l'impact positif de la gouvernance électronique sur la sécurité des données et soulignent l'importance de mesures efficaces pour garantir la protection des informations sensibles.

Limites de la recherche

Malgré les résultats significatifs obtenus, certaines limites de la recherche doivent être prises en compte. Le phénomène de la gouvernance électronique est relativement récent en Algérie, ce que rendent les recherches sur le sujet dans le contexte algérien un peu rares. Ces limites incluent aussi le manque de diversité dans les profils des répondants, la dépendance aux réponses auto-déclarées et la portée limitée de l'étude dans le contexte spécifique d'Algérie Télécom. Ces dernières soulignent la nécessité d'une approche plus large et diversifiée pour une compréhension plus approfondie de l'impact de la gouvernance électronique sur la sécurité des données.

Prolongements possibles de la recherche

Pour étendre les résultats et les implications de cette étude, des prolongements possibles peuvent être envisagés. Il serait bénéfique d'approfondir la recherche en incluant une analyse qualitative pour une compréhension plus nuancée des perceptions des employés. De plus, une comparaison avec d'autres entreprises du secteur des télécommunications pourrait offrir des perspectives supplémentaires sur les meilleures pratiques en matière de gouvernance électronique et de sécurité des données.

RÉFÉRENCES BIBLIOGRAPHIQUES

Banque Mondiale. (2021). *Rapport sur le développement dans le monde chapitre 8, 2021 ,à partir des données du Système et des services de gouvernance des données (DGSS).*

BLANGER Jean-Pierre. (2013). . La non-gouvernance documentaire : quels risques pour l'organisation ? *Documentaliste-Sciences de l'information, 50*(3), p56-57.ISSN : 0012-4508.

Lyotard J.-F. (1995). *La Phénoménologie* (éd. 12e éd.). Paris: PUF.

Piaget J. (1967). *Logique et Connaissance scienti-fique.* Paris: Gallimard.

Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management, 49*(c), 424-438.

Abraham, Rene; Schneider, Johannes; Brocke, vom. (2019). Data governance: A conceptual framework, structured review, and research agenda. (Elsevier, Éd.) *International Journal of Information Management, 49*(c), 424-438.

Abylone. (2020). *Livre Blanc – Collectivités et entreprises : comment engager les acteurs du territoire dans la transformation écologique,Les bonnes pratiques de la gouvernance du numérique.* (ABYLONE, Éd.)

Alenezi, H., Tarhini, A., Masa'deh, R., Alalwan, A., & Al-Qirim, N. (2017). Factors affecting the adoption of e-government in Kuwait: a qualitative study. (E. J. e-Government, Éd.) *15*(2), 84-102.

Aloufi, A. A.; Vasarhelyi, M. A. (2022). The impact of e-government trust components on e-participation in Saudi Arabia. *Government Information Quarterly, 39*(1), 101653.

Al-Rashdi, Y. (2013). E-government security challenges and survey with Indonesian local e-government. *International Journal of Applied Information Systems, 5*(4), 1-6.

Basu, S. (2004). Implementing e-Commerce Tax Policy. *British Tax Review, 1*.

Bentounsi, Mehdi; Cante, Edouad; Coya, Daniel; Darmon, Patrice; Chambourcy, Arnaud; Gnokam, Gisèle. (2019). ARIANE : la Gouvernance des Données comme Accélérateur de Conformité au Règlement Général sur la Protection des

Données. *35 ème Conférence sur la Gestion de Données - Principes,Technologies et Applications.* Lyon, France.

Boughzala, I.; Bououd, I.; Michel, H. (2015). La gouvernance de la sécurité de l'information : concepts et positionnement. . *Revue Internationale d'Intelligence Économique,* 113-136.

Boughzala, I.; Bououd, I.; Michel, H. (2015). La gouvernance de la sécurité de l'information : concepts et positionnement. *Revue Internationale d'Intelligence Économique, 7*(1), 113-136.

Brigitte, G. (2013). . La gouvernance de l'information, point de rencontre complexe entre stratégie ettransversalité. Documentaliste-Sciences de l'information, 2013/3, Vol. 50, p 26-29. ISSN : 0012-4508.

Broster, D.; Misuraca, G.; Bacigalupo, M. (2011). Lifting off Towards Open Government: A Report from the EU Belgian Presidency Conference. *European Journal of e-Practice, 12,* 53-65.

Cárcamo, J., Bernabe, J. B., Navarro, E., Racero, J., & Monreal, V. (2017). Cybersecurity risk management in corporate governance for modern enterprises. *In Proceedings of the 4th International Conference on Information Systems Security and,* (pp. 354-362).

CARPENTIER, Jean-François. (2023). *Livre blanc : La sécurité informatique dans la petite entreprise,Etat de l'art et bonnes pratiques (4e édition).*

Castells, M. (2010). *The Rise of the Network Society* (éd. (2nd ed.). WileyBlackwell.

Centre canadien pour la cybersécurité. (2024). Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B. ITSP.40.111.

Chavan, G. R.; Rathod, M. L. (2009). E-Governance and its Implementation SRELS. *Journal of Information Management, 46*(1), 17-24.

Chen, J. V.; Distler, F. (2019). Understanding information governance and data governance. *ISACA Journal, 4*.

Da Sylva, L., Maurel, D., Bruyère, M., Saint-Germain, M., & Gareau, G. (2019). *cairn.info.* (É. d. communication, Éd.) Consulté le mars 29, 2024, sur https://doi.org/10.4000/edc.8615

Derrar, Hacene. (2023). Transformation numérique en Algérie : Vers un nouveau mode de gouvernance. Quotidien El Watan .

Elana, M. (2023). Expérience client 5.0 : union du digital et de l'humain.

Franco, Jean-Michel. (2018). pourquoi la Banque doit miser sur la gouvernance des données ?

Galvez, Rachel. (2024). Les tendances en matière de gouvernance des données pour 2024.

Gastard, Richard. (2024, Mai 3). Récupéré sur https://www.jedha.co/blog/cybersecurite-quest-ce-que-la-triade-cia

Gavard-Perret, M.-L.; Gotteland, D.; Haon, C.; Jolibert, A. (2012). *Inscrire son projet de recherche dans un cadre épistémologique.* (éd. éd. 2°). (D. M. gestion, Éd.) Paris, France: Pearson.

Groeneveld, Rachid. (2021). Les 6 principaux défis de sécurité du cloud en 2021 » ,. *Security consultant*.

Hashim, Muhammad; Mahfooz, Bakhtawar; Ibrahim, Kainat. (2023). Privacy and Data Security Litigation in Banking: Implications for Corporate Governance. *Journal of Business and Management Research, 2*(2), 655–666.

Heeks, R. (2001). Reinventing Government in the Information Age , dans R. Heeks (dir.) Reinventing Government in the Information Age: International Practice in ITenabled Public Sector Reform,. *London, Routledge*, 9-21.

ITRex. (2023). Récupéré sur https://hackernoon.com/fr/donn%C3%A9es-masquant-comment-elles-peuvent-%C3%AAtre-mises-en-%C5%93uvre-correctement

Jacquier, C. (2008). UrbanGovernance: Forging a PathBetween Complications and Complexity. *Communication présentée au Towards New Territorial Governance.*

Khan, S., Shakil, K. A., & Alam, M. (2020). Cloud computing for e-governance: Aest-practice guide. *In Integrating Cloud Computing Services with IoT Networks*, pp. 180-202.

Koscina, M. (2021). Security and optimization of blockchains and associated algorithms. (U. P. lettres, Éd.) *Cryptography and Security [cs.CR]*.

Kremer-Marietti A. (1993). *Le Positivisme* (éd. 2e éd.). Paris: PUF.

Kshetri, N. (2017). Cybersecurity in a Cyber-Cyber-Cyber World. *IT Professional, 19* (5), 39-43.

LADJIMI, Chokri; MENICACCI, Alexandre. (s.d.). Récupéré sur https://almond.eu/digital-technology-insights/la-gouvernance-de-donnees-votre-passeport-vers-la-creation-de-valeur/

Le Conseil de l'Europe. (2004). Recommandation Rec(2004)15 du Comité des Ministres aux Etats membres.

Légifrance. (2018). LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

Leroy, Philippe. (2021). Que signifie Prévention des fuites de données. *DLP*.

Liem, C.; Petropoulos, G. (2016). (The London School of Economics and Political Science, Éd.) Récupéré sur http://blogs.lse.ac.uk/businessreview/2016/01/19/the-economic-value-of-personal-data-for-online-platforms-firms-and-consumers/

Lio, M. C., Liu, M. C., & Ou, Y. P. (2011). Confiance dans la gouvernance électronique, confiance dans la fourniture de services en ligne ? Les défis de l'administration électronique. *Gouvernement électronique, 5*(4), 324-337.

Lodewijkx, Koos. (2020, novembre). Consulté le mars 28, 2024, sur https://x.com/MidlandInfoSys/status/1713997341558984809

Makhdoom, Imran; Zhou, Ian; Abolhasan, Mehran; Lipman, Justin; Ni, Wei. (2020). PrivySharing: A Blockchain-Based Framework for Privacy-Preserving and Secure Data Sharing in Smart Cities. *Computers & Security*.

Mesaros, Michael. (2020). Consulté le mars 29, 2024, sur oracle.com: https://www.oracle.com/fr/security/databasesecurity/what-is-data-security/#gdpr.

Misuraca, G. (2007). E-Governance in Africa, from Theory to Action: A Handbook on ICTs for Local Governance. *IDRC/Africa World Press*.

Misuraca, G. (2009). E-Government 2015: Exploring m-Government Scenarios, between ICT-driven Experiments and Citizen-centric Implications. *Technology Analysis and Strategic Management, 21*(3), 18.

Misuraca, G. (2010). *Exploratory Emerging ICT-enabled Governance Models in European Cities*. European Commission's Joint Research Centre, Institute for Prospective Technological Studies.

Misuraca, G.; Rossel, P. (2007). Triggering the Governance Perspective of eGovernment Projects: Beyond Mere Digitization of Administration Services, Background paper for the Third Global Knowledge Conference. Kuala Lumpur, 10-13 décembre.

Misuraca, G.; Rossel, P. (2011). Reflexivity, Modelling and Weak Signals of Transformational Tracks to Support Both Micro- and Macro-measuring of Information Society Services. Dans ACM International Conference Proceedings Series (Éd.), *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance (ICEGOV2011)* (pp. 26-28 septembre). Tallinn, Estonia,: ACM Press.

Misuraca, G.; M., Rossel P. et Finger. (2006). Governance with and of ICTs: The Need for New Institutional Design in a Changing World. *Egov Magazine, 2*(5), 36-39.

Misuraca, Gianluca; Viscusi, Gianluigi. (2010). E-Governance for Development: Designing an Operational Roadmap for ICT. (E. P. Reform., Éd.)

Mohr, Maxime. (2022, Mars 27). La Chine présente son plan pour une gouvernance numérique sur fond d'autoritarisme.

Ndou, V. D. (2004). E-government for developing countries: opportunities and challenges. *The electronic journal of information systems in developing countries, 18*(1), 1-24.

OECD. (2014). *Recommandation du Conseil sur la Gouvernance numérique des pratiques de gestion des données des risques de sécurité pour le développement économique et social.* OECD/LEGAL/0415.

OUDIPO. (2014). Quand le document technique devient preuve. *Documentaliste Sciences de l'information, 51*, 41-43.

P., Calhoun. (2001). Consulté le Mars 24, 2024

Plouin, Guillaume. (2022). , *Cloud et transformation digitale - SI hybride, protection des données, anatomie des grandes plateformes* (éd. 6e édition).

Poussing, N., & Dagorn, N. (2012). Engagement et pratiques des organisations en. *17*, 113-143.

Poussing, Nicolas; Dagorn, Nathalie. (2012). Engagement et pratiques des organisations en matière de gouvernance de la sécurité de l'information. *17*, 113-143.

Rusu, L., & Gheorghe, A. (2017). Gouvernance électronique et sécurité des données : défis et implications pour les organisations publiques. *Dans Innovations Administratives pour le Gouvernement Résilient*, pp. 163-183.

Sá, F., Rocha, Á., & Cota P., M. (2016). From the quest for citizens' trust to egovernment service quality monitor. *In Research and Practical Issues of Enterprise*, pp. 253-262.

SERDALAB. (2014). Récupéré sur http://www.serdalab.com/demandedetelechargement/?file=/Medias/Livres%

Sylva, L. D., Maurel, D., Bruyère, M., Saint-Germain, M., & Gareau, G. (2019). (Études de communication) Consulté le mars 29, 2024, sur http://journals.openedition.org/edc/8615

Tikkinen-Piri, C., Rohunen, A., & & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1), 134-153.

Tomo, A.; Todisco, M.; Ruggieri, M.; Vinci, M. B. (2021). Principles and regulations on personal data protection: Compliance through data governance. *Social Sciences, 10*(5), 177.

Triandis, A.; Williams, R. L. (2020). Using cybersecurity frameworks to develop strategies for cybersecurity management. *Journal of Cybersecurity Education, Research and Practice, 4*.

Ullah, F.; Sepasgozar, S. M.; Wang, C. (2019). Challenges and opportunities for implementing e-governance due to lack of citizens' awareness and trust: A case study about Bangladesh. (I. Access, Éd.) *7*, 87785-87800.

Unies, Nations. (2003). *Local Governance Capacity-Building for Full-Range Participation: Concepts, Frameworks, and Experiences in African Countries,*. New York.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). (U. o. Minnesota, Éd.) *Management Information Systems Research Center*, *27*(3), 425-478 .

Zissis, D.; Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583-592.

ANNEXES

ANNEXE A : Questionnaire

L’impact de la gouvernance électronique sur la sécurité des données

Bonjour à toutes et à tous,

Dans le cadre de la préparation de notre mémoire de fin d’études en management Gouvernement électronique à l’Ecole Nationale Supérieure de Management, nous effectuons une étude sur la gouvernance électronique et son impact sur la sécurité des données au sein « d'Algérie Télécom ». A cet effet nous vous prions de nous accorder quelques minutes de votre temps précieux afin de répondre à ce questionnaire.

Nous vous assurons que vos réponses resteront confidentielles et ne seront utilisées qu’a des fins académiques.

Section 1 Fiche signalétique

-Vous êtes ?

Homme

Femme

-Quel âge avez-vous ?

20-29

30-39

40-49

50-59

60 et plus

-Quelle est votre poste au sein d'Algérie télécom ?

Agent de maitrise

Cadre

Cadre supérieur

-Depuis combien de temps travailler-vous chez Algérie Télécom ?

Moins de 5 ans

5-10 ans

11 a 16 ans

17 a 22 ans

Plus de 23 ans

Section 2 Connaissances générales sur la gouvernance électronique et la sécurité des données

-Etes-vous familier avec le concept de gouvernance électronique ?

Oui

Non

-Comment évaluez-vous votre niveau connaissance en matière de sécurité des données et de gouvernance électronique ?

Très faible

Faible

Neutre

Elevé

Très élevé

-Avez-vous reçu une formation sur la sécurité des données et la gouvernance électronique ?

Oui

Non

-Comment évaluez-vous la conformité d'Algérie Télécom aux réglementations en matière de protection des données ?

Très mauvaise

Mauvaise

Neutre

Bonne

Excellente

-Comment évaluez-vous la transparence d'Algérie Telecom en ce qui concerne la gestion et la protection des données personnelles ?

Pas du tout transparente

Peu transparente

Neutre

Transparente

Très transparente

-Comment décririez-vous la culture de la sécurité des données au sein de l'entreprise ?

Très Faible

Faible

Neutre

Forte

Très forte

Section 3 : Mesures de sécurité et pratiques de gouvernance électronique

-Êtes-vous satisfait(e) des mesures de gouvernance électronique mises en place par Algérie Telecom ?

Pas du tout satisfait(e)

Peu satisfait(e)

Neutre

Satisfait(e)

Très satisfait(e)

À quel point faites-vous confiance aux systèmes de sécurité des données mis en place par l'entreprise ?

Pas du tout confiant(e)

Peu confiant(e)

Neutre

Confiant(e)

Très confiant(e)

-Pensez-vous que la gouvernance électronique peut contribuer à réduire les risques liés à la sécurité des données ?

Oui

Non

-Selon vous, quels sont les principaux défis liés à la gouvernance électronique pour garantir la sécurité des données ?

Protection des données personnelles

Sécurité des infrastructures

Sensibilisation et formation

Manque de ressource

Complexité des systèmes

-Dans quelle mesure considérez-vous que la gouvernance électronique des données est importante pour assurer la sécurité des données au sein de l'entreprise ?

Pas du tout important

Peu important

Neutre

Important

Très important

-À votre avis, quelles pourraient être les conséquences d'une mauvaise gouvernance électronique sur la réputation d'Algérie Télécom ?

Perte de clients

Pertes financières

Cyberattaques

Violations de la vie privée

Pannes et interruptions de service

-Trouviez-vous que le nombre d'incidents de sécurité a diminué grâce à la gouvernance électronique?

Oui

Non

-Pensez-vous que les clients d'Algérie Télécom sont conscients des efforts de l'entreprise en matière de gouvernance électronique et de sécurité des données ?

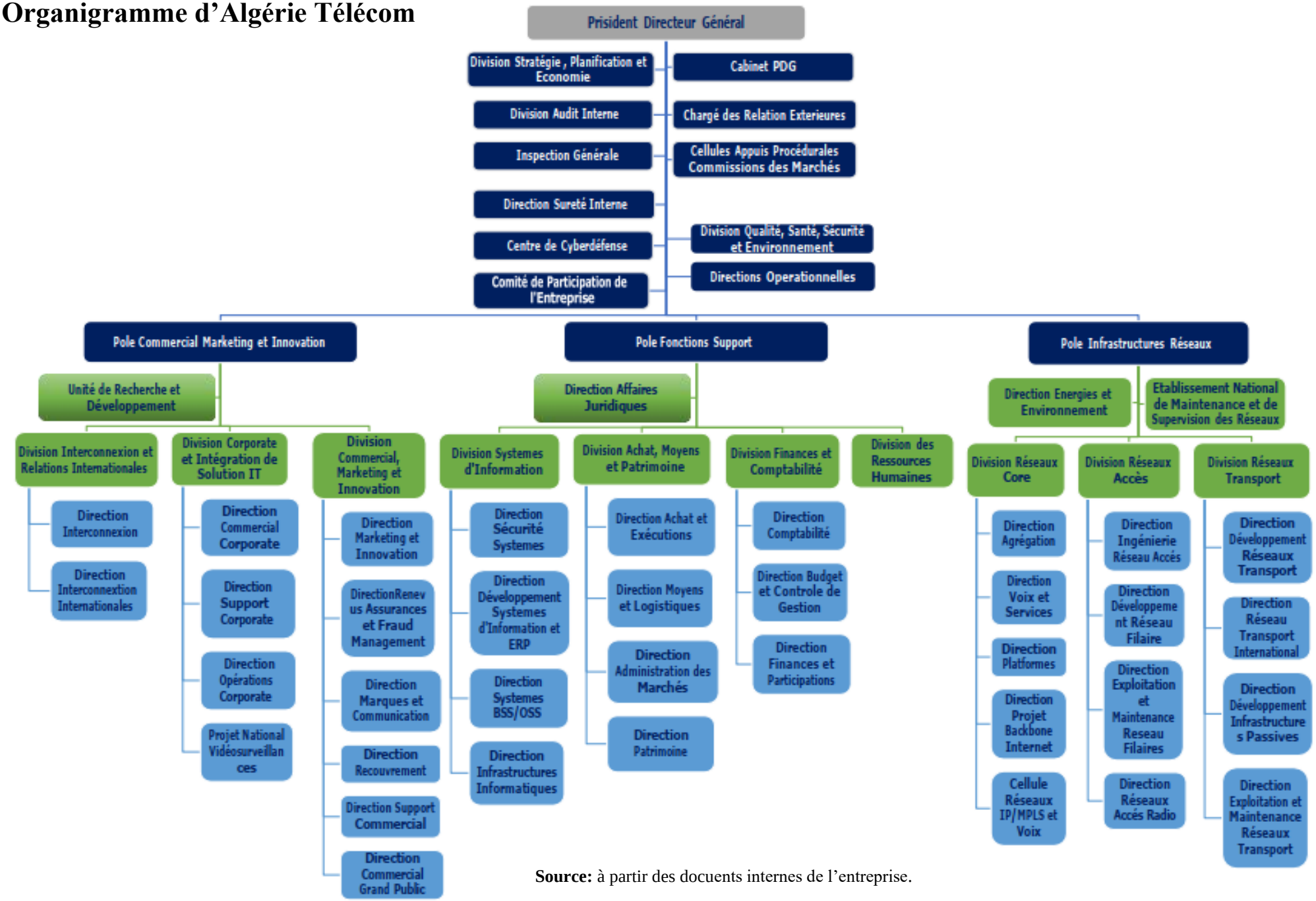
Oui

Non

-Avez-vous des suggestions ou des recommandations pour améliorer la sécurité des données et la gouvernance électronique chez Algérie Télécom ?

ANNEXE B :
Organigramme d'Algérie Télécom

Organigramme d'Algérie Télécom



Source: à partir des docuents internes de l'entreprise.