MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE
ÉCOLE NATIONALE SUPERIEURE DE MANAGEMENT
ENSM. P.U. KOLÉA

MEMOIRE DE MASTER ACADEMIQUE
E-Gouvernement

LES DEFIS LIES A LA CONFIDENTIALITE DES DONNEES DANS LA GOUVERNANCE ELECTRONIQUE : CAS D'ETUDE CNAS TIARET

Elaboré par :

DAHMANI Mostefa

Sous la direction :

Dr. MOHAMED EL HADJ. L

2023/2024

Résumé

Cette étude examine les défis de la confidentialité des données personnelles dans le cadre de la gouvernance électronique, en se concentrant sur la Caisse Nationale des Assurances Sociales (CNAS) Tiaret. À travers une méthodologie qualitative incluant des entretiens directs, elle évalue la manière dont les services numériques de la CNAS assurent la confidentialité des données des assurés. Les résultats révèlent des progrès significatifs dans la digitalisation des services de la CNAS, mais aussi des lacunes persistantes dans la protection des données. Des recommandations sont formulées pour renforcer les politiques de confidentialité, améliorer la formation du personnel et sensibiliser les assurés. En combinant une technologie avancée, une réglementation stricte et une gestion proactive des risques, cette recherche propose des pistes pour une amélioration continue de la gouvernance électronique et de la protection des données dans le secteur public en Algérie.

Mots clés : confidentialité des données, gouvernance électronique, CNAS, services numériques, protection des données.

Abstract : This study examines the challenges of personal data confidentiality within the framework of electronic governance, focusing on the National Social Insurance Fund (CNAS) in Tiaret. Through a qualitative methodology including direct interviews, it evaluates how CNAS's digital services ensure the confidentiality of insured individuals' data. The findings reveal significant progress in CNAS's digital service enhancement, yet persistent gaps in data protection remain. Recommendations are made to strengthen privacy policies, improve staff training, and raise awareness among the insured. By combining advanced technology, stringent regulation, and proactive risk management, this research offers pathways for continuous improvement in electronic governance and data protection in Algeria's public sector.

Keywords: data confidentiality, electronic governance, CNAS, digital services, data protection.

الملخص:

تتناول هذه الدراسة التحديات والمشكلات المتعلقة بسرية البيانات الشخصية في إطار الحوكمة الإلكترونية، مع التركيز على الصـــندوق الوطني للضـــمان الاجتماعي (CNAS) بتيارت. من خلال منهجية البحث النوعي التي تشـمل المقابلات المباشـرة، تقيم الدراسـة كيفية تأمين خدمات الصـندوق الوطني للضـمان الاجتماعي لسرية بيانات المؤمن عليهم. تظهر النتائج تقدماً ملحوظاً في تحديث خدمات CNAS الرقمية، ولكن هناك نقص مستمر في حماية البيانات. تُقدم توصيات لتعزيز سياسات الخصوصية، وتحسين تدريب الموظفين، وتوعية المؤمنين. من خلال الجمع بين التكنولوجيا المتقدمة والتشـــريعات الصـــارمة والإدارة النشـطة للمخاطر، تقترح هذه الدراسـة طرقاً لتحسـين مسـتمر للحوكمة الإلكترونية وحماية البيانات في القطاع العام في الجزائر.

الكلمات المفتاحية: ســـرية البيانات، الحوكمة الإلكترونية، ص و ض إ، الخدمات الرقمية، حماية البيانات.

Remerciement

Tout d'abord, je remercie dieu le tout puissant de m'avoir accordé la volonté, la patience et la force pour accomplir ce travail.

Je tiens à exprimer ma profonde gratitude envers mon encadrante ***: Dr. Leila MOHAMMED EL HADJ****, pour ses précieux conseils et orientations. Sa disponibilité, sa rigueur, sa compétence et sa patience m'ont apporté une aide précieuse dans la réalisation de mon travail.*

Je tiens également à exprimer ma gratitude envers les professeurs et enseignants qui ont accepté de faire partie du jury pour évaluer ce mémoire.

Je tiens à exprimer ma gratitude envers le personnel de la CNAS Tiaret pour leur contribution et leur apport à cette recherche, ainsi que tous les employés de la CNAS qui m'ont apporté leur aide dans la réalisation de mon étude.

Je souhaite exprimer ma gratitude envers l'ensemble du personnel enseignant et administratif de l'ENSM pour les connaissances et les différentes expériences qu'ils m'ont apportées dans ce domaine.

À mes proches, ma conjointe et mes fils.

Tout au long de cette période stressante, je suis reconnaissant envers mes amis et camarades de classe pour leur soutien.

Table des matières

Remerciement ..... **IV**

Liste des tableaux ..... **VIII**

Liste des figures ..... **IX**

Liste des abréviations X

Introduction générale **1**

Chapitre I : Revue de littérature et cadre conceptuel **2**

I.1 Revue de littérature 4

I.1.1 Confidentialité des Données 4

I.1.2 La Gouvernance Électronique 6

I.2 Cadre conceptuel 7

I.2.1 Introduction à la Gouvernance Électronique 7

I.2.1.1 Définition de la Gouvernance Électronique 7

I.2.1.2 Objectifs de la Gouvernance Électronique 8

I.2.1.3 Rôle de la Gouvernance Électronique 8

I.2.1.4 L'évolution de la gouvernance dans le monde 9

I.2.1.5 La gouvernance électronique en Algérie 12

I.2.2 Concepts Clés en Confidentialité des Données 14

I.2.2.1 Données personnelles 14

I.2.2.2 Définition de la Confidentialité des Données 16

I.2.2.3 Concepts de Sécurité des Données 18

I.2.2.4 Les principaux problèmes liés à la confidentialité pour les utilisateurs 19

I.2.2.5 Cadre juridique et réglementaire 20

I.2.2.6 Les prestations de la sécurité sociale à l'ère du numérique 20

I.2.2.7 Création d'une identité numérique vérifiable 21

I.2.2.8 Evaluation des dossiers d'accès aux prestations 21
I.2.2.9 Calcul et paiement des prestations 21
I.2.2.10 Communication entre les organismes de la sécurité sociale et les bénéficiaires 22
I.2.2.11 L'administration publique algérienne en prise avec les TIC 22
II. Chapitre II : Cadre méthodologique et organisationnel 24
II.1 Cadre méthodologique 26
II.1.1 Positionnement épistémologique 26
II.1.2 Approche Méthodologique de la recherche 27
II.1.3 Les outils de collecte des données 28
II.1.3.1 La recherche documentaire : 28
II.1.3.2 Entretiens semi-directif : 28
II.1.4 Traitement et analyse des données 30
II.1.5 Étapes de Traitement des Données d'Entretiens sur NVivo : 30
II.2 Cadre organisationnel 31
II.2.1 Présentation de l'organisme d'accueil (CNAS Tiaret) 31
II.2.1.1 Les missions de la CNAS 32
II.2.1.2 Organisation de la CNAS 33
II.2.1.3 Les structures de la CNAS 33
II.2.1.4 Les bénéficiaires 33
II.2.1.5 Les prestations 34
II.2.2 Les systèmes d'information développés par la CNAS 34
II.2.3 La gouvernance électronique de la CNAS Algérie 35
II.2.3.1 Les services numériques proposés par la CNAS 37
II.2.4 Etat de système de sécurité de la CNAS 39
III. Chapitre III : Présentation et discussion des résultats 41

III.1 Présentation des résultats 43
III.1.1 Présentation de participants interviewé 43
III.1.2 Traitement et analyse des résultats 44
III.1.2.1 Compréhension de la Gouvernance Électronique 44
III.1.2.2 Confidentialité des Données (sensibilisation et défis) 51
III.2 Discussion des résultats 58
III.2.1 Compréhension de la Gouvernance Électronique 58
III.2.2 Confidentialité des Données (sensibilisation et défis) 59
III.2.3 La confidentialité des données dans la gouvernance électronique dans la CNAS60
III.3 Les suggestions : 61
III.4 Les limites de recherche : 62
Conclusion générale 64
Bibliographie 65
Annexes 68

Liste des tableaux

Tableau 1: Les caractéristiques principales des deux paradigmes selon Croom 27

Tableau 2: Quelques détails importants concernant cette cyberattaque sur la CNAS 39

Tableau 3: Attribue interviewé 43

Liste des figures

Figure 1: Répartition géographique des quatre groupes EGDI, 2022 11

Figure 2: Indice de développement de l'e-gouvernement 2022 – par région 12

Figure 3: Indice de développement du gouvernement électronique- Algérie 13

Figure 4: Indice de développement du gouvernement électronique- Algérie (suite)..... 13

Figure 5: Nuage de mots correspondant à la compréhension du Gouvernance Électronique..... 51

Figure 6: Nuage de mots correspondant à la confidentialité des Données (sensibilisation et défis)58

Liste des abréviations

CNAS : Caisse Nationale d'Assurance Sociale

TIC : Technologies de l'Information et de la Communication

EGDI : Indice de Développement de l'E-Gouvernance

AT/ MP : Accidents du Travail et Maladies Professionnelles

ICANN: Internet Corporation for Assigne Names and Numbers

Introduction générale

1 Le contexte de recherche :

Stéphan HARPER disait : « *Bien gérer son entreprise, c'est gérer son avenir et gérer son avenir, c'est gérer son information* »

Aujourd'hui, de nombreuses institutions sont confrontées à des défis en raison de l'arrivée des technologies de l'information et de la communication qui nécessitent des modifications dans leur gestion et leur fonctionnement. L'enjeu est crucial, car ces institutions doivent parvenir à s'adapter à ce changement pour servir mieux les intérêts des différentes parties prenantes internes et externes afin d'instaurer un climat de travail adéquat et une relation de confiance en assurant la confidentialité et la sécurité des données soit personnel ou public. Ce qui permet à l'entreprise de garantir sa performance, sinon son existence sera mise en question.

Dans un contexte où la numérisation des services publics est devenue la norme, la gouvernance électronique apparaît comme un outil crucial pour moderniser l'administration publique. Néanmoins, cette transition vers le numérique pose d'importants défis en matière de protection de la vie privée des individus. En Algérie, la Caisse Nationale des Assurances Sociales (CNAS) constitue un exemple pertinent pour analyser ces défis, en raison de son rôle central dans la gestion des données de santé des citoyens.

2 La question de recherche :

La problématique de cette recherche s'articule autour des défis liés à la confidentialité des données personnelles dans le cadre de la gouvernance électronique de la CNAS.

Est-ce que les services numériques proposés par la Caisse Nationale d'Assurance Sociale en Algérie dans le cadre de la gouvernance électronique, assurent-ils pleinement la confidentialité des données des assurés ?

Pour analyser cette question de manière exhaustive, il est essentiel d'examiner d'abord les sous-questions suivantes :

1. Quels sont les principaux objectifs et principes de la gouvernance électronique ?

2. Quels défis les entreprises envisagent-elles pour assurer la confidentialité des données ?

3. Quelles mesures et stratégies les entreprises mettent-elles en œuvre pour sécuriser les données tout en améliorant l'efficacité des services numériques ?

3 La méthodologie de recherche :

Afin de répondre aux questions soulevées précédemment, nous avons opté pour la méthode qualitative pour d'appréhender toute la complexité.

4 L'objectif de l'étude :

Ce mémoire a pour objectif d'analyser les principaux défis liés à la confidentialité des données personnelles des citoyens assurés auprès de la Caisse Nationale des Assurances Sociales (CNAS) Tiaret, ainsi que la manière dont les assurés font face aux défis liés à l'utilisation des services numériques. L'étude se propose, d'une part, d'analyser les politiques de confidentialité de la CNAS et, d'autre part, d'identifier les axes d'amélioration visant à renforcer la protection des données dans le cadre de la gouvernance électronique en Algérie. À travers une méthodologie d'entretiens directs, cette recherche cherche à établir un diagnostic précis des pratiques actuelles et à formuler des recommandations concrètes. Dans un premier temps, nous clarifions les concepts de gouvernance électronique et de confidentialité des données, puis nous analysons les services publics numériques avant de nous pencher sur la confidentialité des données des services de sécurité sociale, en particulier la CNAS de la Wilaya de Tiaret.

5 Pertinence de la recherche :

5.1 Pertinence managériale :

Cette recherche met en évidence l'importance de la gestion de l'information dans le cadre de la transformation numérique, notamment au sein d'organisations telles que la CNAS en Algérie. L'intégration des technologies de l'information et de la communication (TIC) est cruciale pour optimiser les processus et répondre aux attentes des parties prenantes. Les responsables doivent s'ajuster aux évolutions technologiques afin d'assurer la confidentialité et la sécurité des données, en utilisant la gouvernance électronique comme un moyen d'améliorer l'efficacité

administrative. Cette adaptation est essentielle pour garantir la performance et la durabilité de l'entreprise, tout en maintenant un climat de confiance et en relevant les défis croissants liés à la protection des données personnelles.

5.2 Pertinence scientifique :

Cette étude contribue à la compréhension des impacts de la digitalisation sur les institutions publiques, en se concentrant sur la CNAS en Algérie. Elle fournit des informations précieuses sur la manière dont les technologies de l'information influencent la gestion des données de santé et les défis de confidentialité associés. En explorant ces enjeux dans un contexte spécifique, l'étude enrichit la littérature sur la transformation numérique et la gouvernance électronique. Le cas de la CNAS offre un modèle pertinent pour des recherches futures, aidant à développer de nouvelles approches théoriques et pratiques pour améliorer l'administration publique tout en garantissant la protection des données personnelles.

6 La structure de document :

Ce mémoire est structuré en trois chapitres, chacun abordant un aspect spécifique de la problématique, depuis le cadre théorique jusqu'aux recommandations finales, en passant par l'analyse détaillée du cas de la CNAS Tiaret.

Ce mémoire se répartit en trois chapitres, dans le premier chapitre nous allons présenter une revue de littérature qui représente une recension des écrits ou de la documentation. Ensuite nous abordons le cadre conceptuel où nous allons définir chaque concept étudié avec les éléments clés qui l'entourent, à comprendre : « la gouvernance électronique », « la confidentialité des données ». Dans le second chapitre, nous allons aborder la méthodologie de recherche que nous avons choisie pour notre étude, tel que l'approche méthodologique retenue ainsi que l'outil de collecte de données choisit. Dans le troisième et dernier chapitre, nous allons aborder les résultats et discussion.

Chapitre I : Revue de littérature et cadre conceptuel

L'objet de ce 1er chapitre est de présenter la revue de littérature et le cadre conceptuel relative à la gouvernance électronique de la gestion de la confidentialité dans la CNAS. Pour ce faire, nous allons procéder en deux temps. Dans un premier temps, on va présenter la revue de littérature et le cadre conceptuel qui contient l'ensemble des concepts clés liés à notre thématique, ainsi que à l'Algérie. Dans un second temps, on va exposer la Caisse Nationale d'Assurance Sociale et son système de sécurité.

I.1 Revue de littérature

I.1.1 Confidentialité des Données

La confidentialité des données, aussi connue sous le nom de « protection des informations personnelles », repose sur le principe que chaque individu doit avoir le contrôle sur ses propres données personnelles. Cela inclut le pouvoir de décider comment les entreprises recueillent, stockent et utilisent ces informations. (Matthew Kosinski, 2023) La notion de vie privée individuelle et sa protection ont émergé et évolué dans les sociétés occidentales en parallèle avec le développement des libertés individuelles.

Samuel Warren et Louis Brandeis sont généralement reconnus comme les premiers auteurs à avoir abordé le concept de "vie privée" dans leur célèbre publication de 1890 intitulée "The right to privacy". Ils définissent le droit à la vie privée comme étant le droit d'être laissé seul ("the right to be alone"). Depuis lors, de nombreux auteurs ont tenté de définir ce concept sans parvenir à un consensus juridique clair. Cette difficulté découle en partie de l'extension constante du champ d'application de la vie privée, qui englobe désormais des aspects tels que la vie familiale, la santé, les opinions politiques, philosophie...etc. (Warren, 2010)

Radi Petrov Romansky et Irina noninska (2020), ont developes un article intitulé *« Défis de l'ère numérique pour la confidentialité et la protection des données personnelles »* examine les principaux enjeux liés à la protection de la vie privée et des données personnelles dans le contexte de l'ère numérique. Ils ont mené une étude qualitative basée sur une analyse approfondie de la littérature et des études de cas pour explorer les défis de l'ère numérique pour la confidentialité et la protection des données personnelles. Les auteurs ont analysé un vaste éventail de recherches académiques, de rapports industriels, et de cadres réglementaires, tels que le Règlement Général sur la Protection des Données (RGPD), afin

d'identifier les principaux enjeux et vulnérabilités liés à la collecte, au stockage et à l'utilisation des données personnelles. L'étude examine également des exemples concrets d'entreprises et de gouvernements, mettant en lumière les risques associés aux violations de données et aux cyberattaques. Les résultats de cette analyse soulignent l'importance d'adopter des stratégies robustes de protection des données et de conformité réglementaire pour atténuer les risques et protéger la vie privée des utilisateurs à l'ère numérique.

Naveed Malik (2023) a mené une recherche intitulée *« Stratégies Innovantes : Assurer la Sécurité des Données dans un Paysage Numérique en Évolution ».* Dans cette étude, l'auteur explore les stratégies innovantes que les organisations peuvent adopter pour garantir la sécurité des données à mesure que le paysage numérique continue d'évoluer. Malik utilise une approche qualitative pour analyser les dernières tendances en matière de cybersécurité, en se concentrant sur les technologies émergentes comme l'intelligence artificielle, la blockchain, et l'Internet des objets (IoT). L'étude examine également les meilleures pratiques pour protéger les données contre les menaces croissantes, telles que les cyberattaques sophistiquées et les violations de données. Les résultats de l'étude mettent en évidence l'importance d'une approche proactive en matière de gestion des risques et de mise en œuvre de technologies avancées pour protéger les informations sensibles dans un environnement numérique en constante évolution.

Kabou Salheddine et Sidi Mohamed Benslimane (2017) ont réalisé une thèse intitulée « La gestion de la confidentialité dans le Cloud Computing ». Cette recherche se concentre sur les défis et les stratégies liés à la protection de la confidentialité des données dans les environnements de cloud computing. Les auteurs ont adopté une approche mixte, combinant des analyses théoriques et pratiques pour évaluer les risques associés au stockage et au traitement des données sur des plateformes cloud. Leur étude examine les mécanismes de sécurité actuels, tels que le cryptage, les contrôles d'accès, et les audits de sécurité, tout en identifiant les lacunes et les vulnérabilités potentielles dans ces systèmes. Les résultats soulignent la nécessité d'améliorer les pratiques de gestion de la confidentialité pour renforcer la confiance des utilisateurs dans les services cloud, en recommandant des solutions telles que l'authentification multi-facteurs, la surveillance continue, et l'adoption de politiques de confidentialité rigoureuses.

I.1.2 La Gouvernance Électronique

Dans le deuxième volet de notre thème, nous abordons la gouvernance électronique, où une précision terminologique s'impose concernant les concepts d'administration électronique, « e-gouvernance », et « gouvernement électronique ».

Selon Benyekhlef dans "L'administration publique en ligne au Canada" (2004), « La mise en place d'un gouvernement en ligne nécessite diverses composantes, parmi lesquelles figure l'administration électronique, qui se définit comme la prestation électronique de services ». Mylène Ramm, citée par Bal (2005), affirme que l'administration électronique implique trois familles d'acteurs : le G to B (Government to Business), le G to C (Government to Citizen) et le G to G (Government to Government). (Benyekhlef, 2004)

Quant au gouvernement électronique, la définition de Boudreau (2011, p. 340) le décrit comme « *l'utilisation des nouvelles technologies de l'information par des organisations publiques afin de les soutenir dans leur fonctionnement interne ainsi que dans leurs relations avec diverses clientèles et avec d'autres organisations* »

Le concept de gouvernement électronique implique initialement la mise à disposition en ligne d'informations publiques telles que les lois, les données relatives à la santé, à l'éducation et à l'économie. Ensuite, il cherche à numériser les processus administratifs en offrant aux utilisateurs la possibilité de les effectuer via Internet (Ossama, 2001). Les utilisateurs auront la possibilité de compléter des formulaires en ligne, de soumettre leur déclaration de revenus, d'obtenir un extrait de registre de commerce ou encore de solliciter une assistance sociale de la part de l'État.

Le gouvernement électronique n'est pas simplement une question technique, mais il est considéré comme « Un outil de grande importance stratégique pour améliorer la prestation de services aux citoyens ». Les éléments constitutifs de l'e-gouvernance comprennent l'e-administration, qui concerne la fourniture électronique de services aux citoyens et aux administrations, l'e-société, qui vise à répondre aux besoins sociétaux des citoyens à travers des services numériques, et l'e-démocratie, qui implique la participation directe des citoyens à la vie politique. Néanmoins, leur étude s'est focalisée exclusivement sur l'administration électronique. (Brown D. , 2005)

I.2 Cadre conceptuel

I.2.1 Introduction à la Gouvernance Électronique

La gouvernance électronique (ou e-gouvernance) est un domaine qui utilise les technologies de l'information et de la communication (TIC) pour améliorer la prestation des services publics, la transparence et la participation citoyenne. Pour comprendre ce concept clé on va voir les éléments suivants :

I.2.1.1 Définition de la Gouvernance Électronique

Concernant ce nouveau concept, de multiples définitions de l'E-gouvernement ou gouvernement électronique ont été élaborées par des chercheurs et d'importantes organisations internationales. Ces définitions se distinguent par l'objectif attendu de ce modèle de gouvernance.

L'Organisation de Coopération et de Développement Économiques (OCDE) propose une définition utilitariste de l'e-gouvernement. Dans cette optique, l'E-gouvernement implique l'utilisation des technologies de l'information et de la communication pour améliorer la gestion des affaires publiques. (ocde, 2013)

Selon le département des affaires économiques et sociales des Nations Unies (UNDESA), l'E-gouvernement est défini comme un gouvernement qui utilise les technologies de l'information et de la communication (TIC) afin de réorganiser ses interactions tant internes qu'externes. (Nations Unies, 2022)

Selon Sunny et James, le concept d'E-gouvernement se réfère à la prestation de services gouvernementaux courants et à la diffusion d'informations en utilisant des moyens électroniques, en particulier ceux exploitant les technologies Internet, que ce soit à domicile, au travail ou via des kiosques publics. (Sunny & James, 2003)

Le concept de gouvernement électronique englobe toutes les fonctions et opérations administratives qui s'appuient sur les technologies de l'information et de la communication (TIC). Il couvre les quatre secteurs de la gouvernance et de l'administration publique : les politiques économiques et sociales de l'État, ses interactions avec les citoyens et l'État de

droit (la démocratie électronique), ses processus internes et ses relations avec la communauté internationale. (Brown, 2005)

En dépit de la diversité des définitions et des objectifs associés à la transformation numérique et à l'adoption du modèle d'E-gouvernement, il est observé que ce concept demeure centré sur l'utilisation des technologies de l'information et de la communication dans la fourniture des services publics, ainsi que sur l'amélioration des interactions avec les usagers de l'administration publique.

I.2.1.2 Objectifs de la Gouvernance Électronique

Les cinq principes de base des objectifs du gouvernement électronique, selon l'ONU sont :

- Proposer des services répondant aux choix des citoyens ;
- Améliorer l'accessibilité du gouvernement et de ses services ;
- Promouvoir l'inclusion sociale ;
- Fournir des informations de manière responsable (Alain, 2005).

Ce modèle électronique gouvernemental offre de multiples avantages tant pour les utilisateurs que pour l'administration publique, qui peuvent être résumés comme suit :

- La réduction des coûts et des dépenses grâce à l'adoption des technologies de l'information et de la communication ;
- La célérité dans l'exécution des opérations, entraînant ainsi des gains de temps, contrairement au traitement manuel qui dépend de l'intervention humaine et nécessite plus de temps pour être effectué ;
- La fourniture de services de haute qualité. Le gouvernement électronique garantit une communication de haute qualité et une transparence de l'information ;
- La créativité et l'innovation dans la prestation de services. En réalité, le concept de gouvernement électronique contraint les organismes gouvernementaux à maintenir leur technologie à jour et à rechercher en permanence des solutions novatrices pour améliorer les services publics. De plus, il est essentiel de procéder régulièrement à la révision et à la simplification des lois et des réglementations ;

- La promotion de l'engagement citoyen dans l'élaboration des stratégies et des politiques publiques ;
- L'évolution de la e-démocratie implique l'emploi du courrier électronique pour interagir avec les représentants élus, pour voter en ligne et pour assister aux réunions officielles par le biais de la technologie des téléconférences. Cette approche favorise une plus grande participation du public aux affaires gouvernementales.
- La contribution au développement économique est de plus en plus déterminée par l'accès à l'information et l'utilisation de la technologie afin d'améliorer la prestation des services, étant donné que l'économie repose de plus en plus sur ces éléments. L'importance de la technologie dans la croissance économique sera grandement renforcée par la mise en place du gouvernement électronique.

I.2.1.3 Rôle de la Gouvernance Électronique

- Prestation de Services Publics : L'e-gouvernance facilite l'accès aux services tels que les impôts, les permis, les soins de santé et l'éducation.

- Prise de Décision : Elle fournit des données en temps réel pour aider les décideurs à formuler des politiques efficaces.

- Inclusion Numérique : L'e-gouvernance vise à réduire la fracture numérique en garantissant que tous les citoyens ont accès aux services en ligne.

I.2.1.4 L'évolution de la gouvernance dans le monde

Le rôle que joue le gouvernement au sein de la société évolue de manière rapide et continuelle. Cette évolution semble s'être accélérée au cours des vingt dernières années, principalement en raison de l'adoption massive des technologies de l'information et des processus de libéralisation des États et de mondialisation de l'économie. Subissant de plus en plus de pressions, les gouvernements doivent redéfinir leurs activités dans des domaines où ils étaient jusqu'à maintenant directement impliqués, comme les services publics, l'éducation ou la santé. Cette tendance est désormais influencée par la crise financière, par certains échecs liés à des privatisations ainsi que par l'émergence de certaines nouvelles

approches, issues en particulier de pays en développement tels que ceux de la zone BRICS[1] , mais également des États-Unis. On est en droit de s'interroger sur l'avenir de l'externalisation des prestations de services, qui pourrait se poursuivre ou prendre de nouvelles formes (Misuraca, 2011).

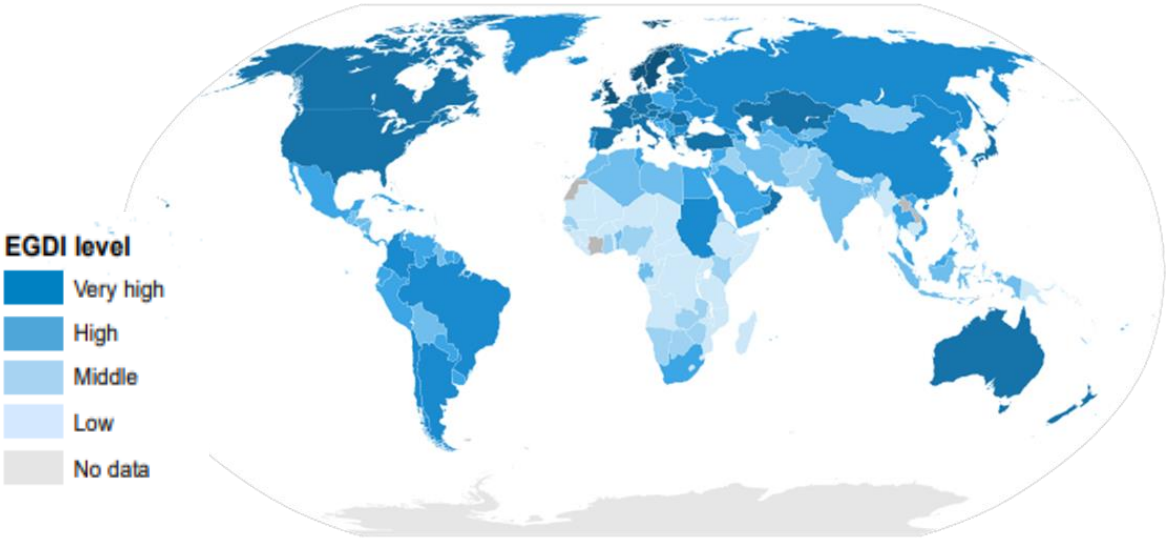
Les gouvernements disposent des systèmes les plus avancés de l'histoire en ce qui concerne les technologies de l'information et de la communication (TIC). Ils bénéficient de réseaux étendus et d'une puissance de calcul sans précédent. Cependant, ils font face à un paradoxe : bien qu'ils soient capables d'accumuler d'énormes quantités d'informations, ils éprouvent toujours des difficultés à les traiter afin d'en obtenir une meilleure compréhension, à prendre des mesures efficaces ou à résoudre leurs principaux problèmes. (Misuraca, 2011).

Le rapport sur la gouvernance électronique pour l'année 2022, récemment publié par le Département des affaires économiques et sociales des Nations Unies, met en avant les initiatives des États membres en matière de transformation numérique. Cette douzième édition offre un aperçu de l'évolution de l'e-Gouvernement dans les 193 États membres et évalue les avancées réalisées dans l'adoption des technologies de l'information et de la communication par les gouvernements. Réalisée tous les deux ans, cette enquête permet d'évaluer les pratiques numériques des gouvernements en termes de transparence, d'inclusion, d'efficacité et d'efficience, tout en fournissant des données statistiques actualisées sur l'utilisation des TIC par les administrations publiques. En outre, cette étude classe les pays membres en fonction de l'indice de développement de l'e-Gouvernement (EGDI) voir annexe B.

Cette enquête 2022 répartit les pays en 4 catégories selon le développement de l'e-gouvernement (très élevé, élevé, intermédiaire et faible).

[1] Cinq pays forment la zone BRICS : le Brésil, la Russie, l'Inde, la Chine et l'Afrique du sud.

Figure 1: Répartition géographique des quatre groupes EGDI, 2022



Source : United Nations E-Government Survey, 27 September 2022.

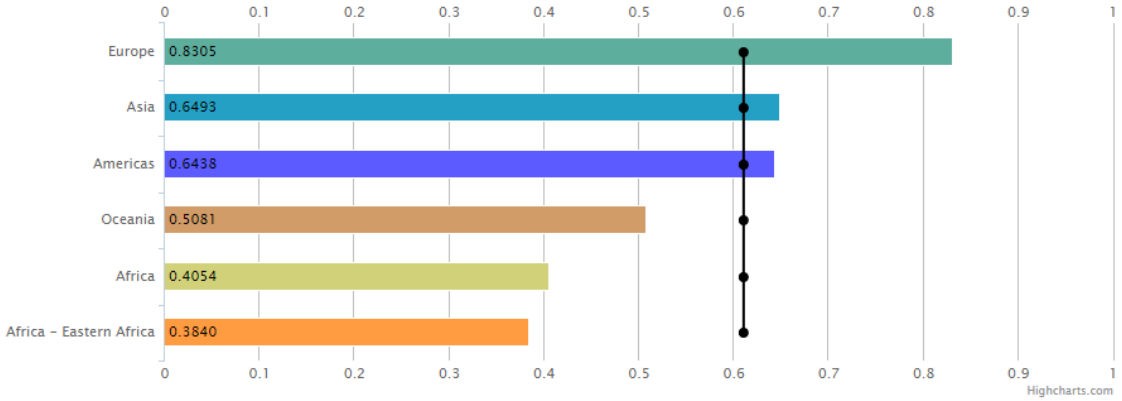
Sur un total de 193 pays ciblés par l'enquête, il ressort que :

- 60 pays ont des valeurs d'EGDI très élevées allant de 0,75 à 1,00 ;
- 73 pays ont des valeurs élevées de 0,50 à 0,75 ;
- 53 pays font partie du groupe intermédiaire de l'EGDI avec des valeurs comprises entre 0,25 et 0,50 ;
- Sept pays ont de faibles valeurs d'EGDI (0,00 à 0,25).

Le Danemark, la Finlande et la Corée du Sud sont en tête de liste. Les Emirats Arabes Unis sont l'un des pays les plus développés du monde arabe avec un EGDI de 0,901(United Nations E-Gouvernement Survey, 2022).

Le rapport indique également que l'Afrique est en deçà des autres continents avec un EGDI inférieur à la moyenne mondiale :

Figure 2: Indice de développement de l'e-gouvernement 2022 – par région



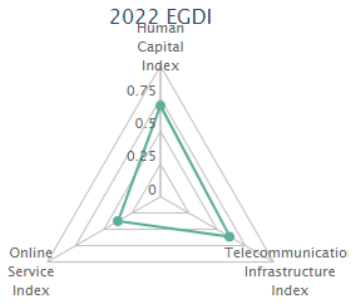
Source : 2022 United Nations E-Government Survey, consulté le 22-04-2024

I.2.1.5 La gouvernance électronique en Algérie

Depuis plusieurs années, l'Algérie a entrepris des démarches visant à promouvoir la gouvernance électronique, notamment à travers l'adoption d'une stratégie nationale. La Stratégie nationale de l'e-gouvernance 2014-2020 a été mise en place afin de définir les orientations et les objectifs du développement de l'e-gouvernance en Algérie. Cette initiative s'est concrétisée par la création d'infrastructures essentielles telles que le réseau national de fibre optique et le portail national d'e-gouvernance.

Cette stratégie a mené l'Algérie parmi les pays du groupe 2 (EGDI élevé) avec un indice de développement du e-Gouvernement de 0.5611, elle est classée 112ème sur 193 pays et la 9ème place en Afrique, donc elle a gagné 8 positions par rapport au classement de 2020 (Tadjeddine, 2023).

Figure 3: Indice de développement du gouvernement électronique- Algérie

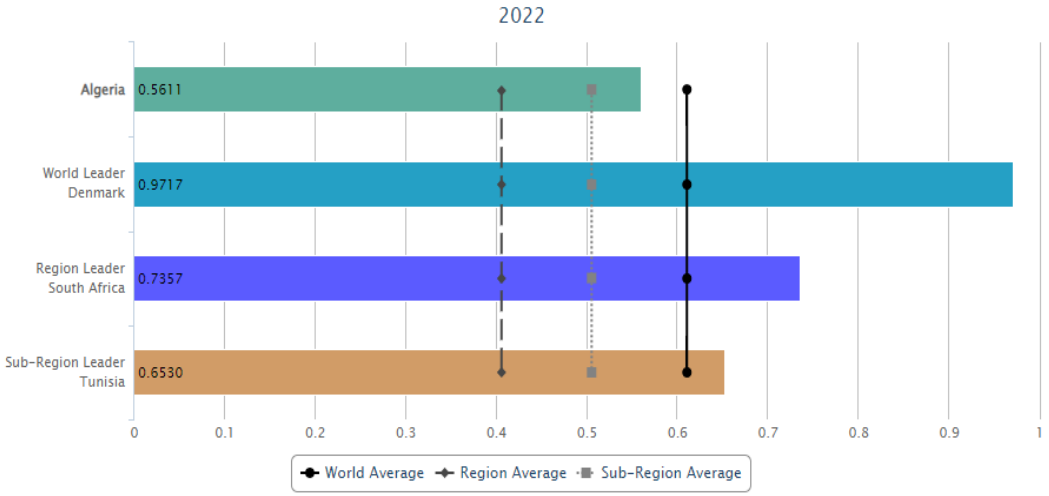


Gouvernement électronique (IDEG 2022 : 0,5611)	
Classement 2022	112
Groupe	HEGDI
Classe de notation	H2
Classement 2020	120
Changement	-8

Participation électronique (EPART 2022 : 0,2273)	
Classement 2022	148
Classement 2020	183
Changement	-35

Source : United Nations E-Gouvernement Survey, consulté le 22-04-2024

Figure 4: Indice de développement du gouvernement électronique- Algérie (suite)



Source : United Nations E-Gouvernement Survey, consulté le 22-04-2024

Malgré ces réalisations, la gouvernance électronique en Algérie est encore confrontée à plusieurs défis :

Fracture numérique : L'accès à internet et aux TIC reste inégal en Algérie, ce qui limite l'utilisation des services en ligne par les citoyens.

Compétences et formation : Le manque de compétences et de formation en matière d'e-gouvernance est un obstacle majeur au développement de ce domaine.

Bureaucratie et résistance au changement : La résistance au changement au sein de l'administration publique peut freiner l'adoption de nouvelles technologies et de nouveaux processus.

Sécurité et confidentialité des données : La protection des données personnelles et la sécurité des systèmes informatiques sont des enjeux majeurs de l'e-gouvernance.

I.2.2 Concepts Clés en Confidentialité des Données

I.2.2.1 Données personnelles

Conformément au Règlement Général sur la Protection des Données (RGPD), une donnée personnelle désigne toute information se rapportant à une personne physique identifiée ou identifiable. Cette définition englobe non seulement des éléments explicites tels que le nom et le prénom, mais également des informations indirectes telles qu'un numéro de téléphone, une adresse postale, ou encore des données biométriques telles que la voix ou l'image d'une personne. En d'autres termes, il s'agit de toute information permettant d'identifier ou de relier directement (par exemple, par le nom) ou indirectement (par exemple, par un numéro de téléphone ou une adresse) une personne spécifique. Cette identification peut résulter de l'utilisation d'une seule donnée ou de la corrélation de plusieurs données.

I.2.2.1.1 Enjeux Des Données Personnelles

- **Enjeux économiques**

Avant d'aborder en profondeur notre sujet, il convient de mettre en avant l'importance des données personnelles de nos jours, notamment dans le domaine commercial. L'adage bien connu "Si c'est gratuit, c'est vous le produit" reflète la réalité de l'environnement en ligne actuel. Avec la monétisation croissante des données, un marché des données personnelles s'est développé, certains allant jusqu'à le qualifier de "nouvel or noir" du 21ème siècle. Le phénomène du "Big data" accentue la capacité de stockage et d'échange de données pour les entreprises. Ainsi, une logique économique s'est progressivement mise en place : l'entreprise qui collecte le plus d'informations sur les consommateurs serait en meilleure position pour les influencer. (BELLEIL, 2011). Il est inévitable que ce postulat soulève, en plus des interrogations sur le droit de la vie privée, des

interrogations sur le droit de la concurrence en ce qu'il permet à l'entreprise de posséder un pouvoir de marché. Dans le domaine du commerce en ligne, le marketing ciblé vise à adapter les offres aux clients de manière plus durable afin de les fidéliser. La pratique des cookies en est le meilleur exemple. Deux grands paradigmes sont en opposition dans cette révolution de l'information : d'une part, la liberté de l'échange et du commerce, et d'autre part, le respect de la vie privée. En Europe et aux États-Unis, des études ont mis en évidence l'inquiétude et la méfiance des consommateurs vis-à-vis des pratiques du commerce en ligne (FRAYSSINET, 2013).

Les récentes affaires qui révèlent des scandales spécifiques à des plateformes telles que Facebook ou Google, suscitent des inquiétudes chez les utilisateurs d'internet. La gestion des informations personnelles recueillies en ligne avec des objectifs économiques sous-jacents pose un souci. Le droit doit intervenir afin de réguler ces pratiques et prévenir les abus. Il est aussi important pour les entreprises de prendre en compte ces concepts de droit au respect de la vie privée, en particulier dans le but de créer un climat de confiance durable avec leurs clients.

- **Enjeux politiques et sociétaux**

En plus des problèmes économiques évidents liés à l'utilisation des données personnelles, il y a aussi des problèmes politiques et sociétaux. Les techniques de surveillance sont souvent associées à des moyens politiques d'asservissement du peuple (RAGOUCY, 2010). De nombreux écrits littéraires font référence à cette problématique, notamment le célèbre roman d'anticipation de George Orwell, "1984", décrivant une société sous le contrôle omniprésent de Big Brother. Ce roman est fréquemment évoqué, parfois de manière excessive, afin de nous sensibiliser aux risques potentiels liés à la manipulation de nos données personnelles dans nos sociétés contemporaines. Par exemple, les informations obtenues à partir de notre géolocalisation ou les technologies de reconnaissance faciale pourraient être détournées afin d'instaurer un contrôle permanent sur les individus.

Dans le même ordre d'idées, Michel Foucault, dans « Surveiller et punir », analyse le panoptique imaginé par Bentham au 19ème siècle comme une technique permettant la surveillance la plus efficiente et la plus complète possible des prisonniers (THIRION, 2011).

Le procédé présente l'avantage d'assurer un anonymat total, de sorte que les détenus demeurent dans l'incertitude quant à leur surveillance. L'architecture virtuelle créée par le World Wide Web (W.W.W.) peut être considérée comme la réalisation à l'échelle mondiale du concept de panoptique développé par Bentham. Les nouvelles technologies de traitement massif de données (Big Data) permettent non seulement la surveillance des individus, mais également l'accès à leurs pensées les plus intimes, souvent sans leur consentement. Cependant, ces données extraites s'avèrent également précieuses pour la prévention de diverses formes de criminalité. En Europe, la promotion de la coopération policière et judiciaire favorise l'échange d'informations telles que les empreintes digitales ou les numéros d'immatriculation des véhicules (CASTETS-RENARD, 2015).

Dans ce contexte, la protection des données personnelles est réduite, car l'accent est mis sur l'intérêt collectif au détriment de l'intérêt individuel. Cela se traduit par une exemption de certaines dispositions de la réglementation européenne en ce qui concerne les traitements de données à caractère personnel à des fins de sécurité publique. De plus, les banques sont particulièrement impactées par la législation sur la protection des données, car elles sont tenues de jouer un rôle proactif dans la prévention du blanchiment d'argent et du financement du terrorisme.

I.2.2.2 Définition de la Confidentialité des Données

La confidentialité des données se réfère à la protection des informations sensibles contre tout accès, utilisation ou divulgation non autorisés. Cela inclut les données personnelles, médicales, financières et autres informations confidentielles.

Selon (Terranova, 2021), la confidentialité des données fait prévaloir les droits individuels. Elle tient compte de la façon et des raisons pour lesquelles les données sont recueillies, traitées, partagées, stockées et supprimées, conformément aux réglementations régionales ou sectorielles. Elle englobe également les préférences de confidentialité choisies par les utilisateurs et la façon dont les organisations gèrent les informations personnelles. Dans le présent contexte, les informations personnelles désignent tous les éléments de données qui, seuls ou en combinaison, peuvent être utilisés pour identifier un individu, par exemple son nom, son adresse et ses coordonnées. Il peut également s'agir de toute donnée liée à une

action effectuée en ligne ou hors ligne, comme l'attribution d'une mention « J'aime », un partage sur les médias sociaux ou les détails d'une transaction financière. (Terranova, 2021)

I.2.2.2.1 Guide de la Conformité à la Confidentialité des Données

Le paysage de la confidentialité des données est complexe et il continue d'évoluer. Il présente de nombreux défis pour les organisations en créant incertitude à plusieurs niveaux quant à savoir si, comment et quand traiter les données personnelles. Le mise en œuvre complexe du RGPD et les efforts continus dans le monde entier pour rédiger les réglementations sur la confidentialité des données ont un sérieux impact sur les capacités des organisations à mettre à jour et aligner leurs pratiques commerciales sur les exigences réglementaires en constante évolution. Nous avons rassemblé cette confidentialité des données Manuel pour tenter de simplifier les exigences et vous aider à démarrer la confidentialité de vos données parcours de conformité. La boîte à outils contient informations et ressources utiles pour vous aider vous évaluez vos processus commerciaux actuels contre les meilleures pratiques en matière de confidentialité des données et prendre les mesures nécessaires pour les améliorer.

Cette boîte à outils reflète les meilleures pratiques alignées sur les exigences du RGPD, exigences et pratiques spécifiques au Moyen Région Est et propriété exclusive de PwC cadres. La boîte à outils convient à tous les organisations traitant des données personnelles et à la recherche d'une approche pratique pour construire leurs programmes de confidentialité des données, que ce soit pour se conformer avec les réglementations en matière de confidentialité ou pour devenir compétitif avantage.

I.2.2.2.2 Dimensions de la Confidentialité des Données

- **Confidentialité de l'Accès :** Empêcher l'accès non autorisé aux données.
- **Confidentialité de la Transmission :** Protéger les données pendant leur transfert (par exemple, via des protocoles de chiffrement).
- **Confidentialité du Stockage :** Sécuriser les données lorsqu'elles sont stockées dans des bases de données ou des systèmes.

I.2.2.2.3 Principes et Normes Internationaux

RGPD (Règlement Général sur la Protection des Données) : Adopté par l'Union européenne, il définit les droits des individus concernant leurs données personnelles et impose des obligations aux organisations qui les traitent.

Loi sur la Protection des Données Personnelles : Chaque pays a ses propres lois pour protéger la vie privée des citoyens.

I.2.2.3 Concepts de Sécurité des Données

Chiffrement : Convertir les données en un format illisible sans la clé appropriée.

Authentification : Vérifier l'identité d'un utilisateur avant d'accéder aux données.

Gestion des Accès : Contrôler qui peut accéder aux données et à quel niveau.

Bien que la sécurité des données et la protection de la vie privée soient distinctes, elles sont toutes deux des composantes de la protection des données, un concept englobant notamment la confidentialité et la sécurité des données.

La protection des données vise à restreindre l'accès non autorisé, l'utilisation inappropriée et la divulgation des données, en mettant en place des politiques, des procédures et des technologies pour assurer la confidentialité, l'intégrité et la disponibilité des données.

La préservation de la confidentialité des données s'inscrit dans le cadre plus général de la protection des données, en se focalisant sur la prévention de l'accès et de la divulgation non autorisés de données personnelles et sensibles. Les entreprises peuvent ainsi garantir le respect de la vie privée des individus et maintenir la confidentialité des informations délicates en assurant la sécurité des données (Veritas, 2022).

I.2.2.3.1 Pourquoi la confidentialité des données est-elle importante ?

Dans plusieurs pays, la confidentialité des données est considérée comme un droit fondamental et est protégée par une réglementation régionale ou sectorielle. Par exemple, l'Union européenne a mis en place le Règlement général sur la protection des données (RGPD) tandis que les résidents de la Californie, aux États-Unis, sont visés par la California Consumer Privacy Act (CCPA). Les organisations qui adoptent des pratiques de

confidentialité des données rigoureuses et transparentes peuvent établir avec leur clientèle un lien de confiance basé sur la façon dont elles traitent, entreposent et partagent les données d'utilisateurs (Terranova, 2021).

Si les données privées ne sont pas sécurisées, ou si les utilisateurs n'ont pas de contrôle sur la façon dont leurs données sont utilisées, les informations personnelles peuvent être vendues à des annonceurs publicitaires sans consentement. Pire encore, elles peuvent être exposées à une violation de données et utilisées par des pirates pour mener des activités malveillantes.

I.2.2.4 Les principaux problèmes liés à la confidentialité pour les utilisateurs

Le suivi ou surveillance en ligne, les activités en ligne font régulièrement l'objet d'un suivi, le plus souvent à l'aide de témoins. Ceux-ci permettent d'enregistrer les actions effectuées par les utilisateurs sur leur navigateur Web. Plusieurs pays ont légiféré pour exiger des organisations qu'elles informent les utilisateurs de l'utilisation de témoins et leur demandent d'accepter ce niveau de suivi des données. Toutefois, la surveillance en ligne peut également limiter considérablement la liberté d'expression (Terranova, 2021).

Le manque de transparence dans les politiques de confidentialité même si elles sont facilement accessibles aux utilisateurs sur la plupart des sites web ou applications, les politiques de confidentialité utilisent souvent des termes compliqués qui peuvent être difficiles à comprendre. Par conséquent, les utilisateurs ne saisissent pas toujours clairement comment les informations personnelles qu'ils fournissent pour accéder à un service en ligne, comme leur adresse courriel ou leur numéro de téléphone, seront recueillies, utilisées, stockées ou partagées (Terranova, 2021).

La perte de contrôle sur les données, s'il y a un manque de transparence dans la communication de la politique, il est possible que les utilisateurs n'aient que peu ou pas de contrôle sur leurs données personnelles ou leur droit d'être laissé seul. Dans ce cas, ils n'ont aucun mot à dire sur la manière dont leurs informations sont partagées au-delà du site Web ou du service en ligne en question, ou sur la manière dont leurs données sont traitées et enregistrées (Terranova, 2021).

I.2.2.5 Cadre juridique et réglementaire

L'Algérie quant à elle a dû attendre jusqu'en 2018 pour se doter de son propre arsenal juridique à travers la promulgation de la Loi 18-07 du 10 juin 2018 (Journal officiel n°34 du 10 juin 2018).

Cette Loi comme l'indique l'article 1 a pour objet de fixer les règles de protection des données personnelles qui se traduisent par l'ancrage de nouveaux principes la consécration de nouveaux droits et la mise en place de nombreuses obligations.

Dans cette dynamique, l'année 2020, fut l'année de constitutionnalisation du principe de protection des données à caractère personnel à travers la nouvelle disposition introduite par la constitution algérienne. Ce qui constitue un acte fort en vue de soutenir l'approche mise en place en relation avec de la protection des données à caractère personnel.

A cet effet, cette modeste contribution tend à défraichir et apporter certains éclaircissements sur les contours de la loi algérienne relative à la protection des données personnelles, tout en signalant le pointillisme et la technicité des dispositions introduite ce qui impose un minimum de savoir technique pour pouvoir cerner les contours de cette loi.

I.2.2.6 Les prestations de la sécurité sociale à l'ère du numérique

La sécurité sociale est un mécanisme de protection sociale qui repose sur des transferts financiers destinés à prévenir la précarité et l'insécurité au sein d'une communauté, contribuant ainsi à promouvoir la cohésion sociale.

Avec l'avènement du numérique, les organismes de sécurité sociale ont modernisé la prestation de leurs services à toutes les étapes, de la réception du courrier à la lutte contre la fraude. Parmi ces avancées, on peut mentionner la numérisation des données des bénéficiaires des prestations de sécurité sociale, la dématérialisation des interactions entre les administrateurs et les usagers, l'implication de ces derniers dans la production de services via le développement des services en ligne, ainsi que le calcul automatisé des droits et des prestations (traitement automatisé des dossiers). De plus, des outils d'intelligence artificielle sont employés pour faciliter la détection des dossiers présentant des risques.

I.2.2.7 Création d'une identité numérique vérifiable

Il est essentiel d'avoir une identité numérique vérifiable afin de solliciter et de bénéficier de services. De plus, elle joue un rôle crucial dans la reconnaissance des droits et la possibilité de contester un refus de prestation. Du point de vue des organismes publics, une identité numérique vérifiable permet de prévenir les cas de doublons et de fraudes, de faciliter un ciblage précis et d'accroître l'efficacité des services (Tavits & Sargsyan , 2022) .

L'intégration des technologies d'intelligence artificielle a effectivement contribué à renforcer la lutte contre la fraude en évaluant les dossiers soumis à l'aide de critères établis par les spécialistes du domaine. La capacité à croiser des informations provenant de diverses sources permet de détecter les fraudes et les anomalies chez les bénéficiaires de l'aide sociale.

La création d'une identité numérique pour l'ensemble des bénéficiaires présente l'avantage de diminuer les coûts pour toutes les parties impliquées (citoyens, États, entreprises). Un autre avantage de l'identité numérique est de renforcer l'inclusion financière en offrant un accès aux services de sécurité sociale à tous les segments de la population. Néanmoins, la question de la sécurité des données personnelles reste un enjeu crucial, comme souligné précédemment.

I.2.2.8 Evaluation des dossiers d'accès aux prestations

Divers pays utilisent des technologies numériques pour évaluer l'éligibilité aux prestations sociales. Un exemple notable est celui du Canada, plus précisément dans la province de l'Ontario, où les décisions d'admissibilité sont automatisées depuis 2014 grâce au Système de gestion de l'aide sociale. Ce logiciel, basé sur la technologie standard IBM et personnalisable, est également déployé dans des programmes similaires en Australie, en Allemagne, en Nouvelle-Zélande et aux États-Unis (Tavits & Sargsyan , 2022). Le travail fastidieux d'évaluation des dossiers d'accès longtemps réalisé par les agents d'État est désormais automatisé dans de nombreux pays développés.

I.2.2.9 Calcul et paiement des prestations

Les organismes compétents recourent aux technologies numériques pour le calcul et le versement des prestations sociales, de manière automatisée. Cette approche présente l'avantage indéniable

d'optimiser l'efficacité et de réduire les coûts, bien que des risques d'erreurs subsistent, nécessitant ainsi des vérifications régulières de la part des employés (Refafa.b, 2020) .

I.2.2.10 Communication entre les organismes de la sécurité sociale et les bénéficiaires

Les interactions traditionnelles en face-à-face, par téléphone ou par courrier sont de plus en plus fréquemment remplacées par des interactions en ligne. Néanmoins, des préoccupations concernant la sécurité des communications ont émergé, ainsi que des défis liés à l'absence d'accès à Internet et/ou de compétences numériques. Ces problématiques sont exacerbées par la complexité des portails en ligne, ce qui peut entraîner une privation des droits des demandeurs aux services de la sécurité sociale (Refafa.b, 2020).

I.2.2.11 L'administration publique algérienne en prise avec les TIC

Afin de s'adapter à un environnement en constante évolution, l'administration publique en Algérie met progressivement en place les technologies de l'information et de la communication, perçues comme un levier d'amélioration des services publics. En 2009, les autorités ont lancé le programme "e-Algérie 2013" dans le but d'intégrer l'Algérie dans l'économie numérique. Toutefois, en raison des retards accumulés dans sa mise en œuvre, le projet a été rebaptisé "e-Algérie" sans date butoir. Ce plan repose sur treize axes principaux, chacun étant assorti d'objectifs spécifiques et d'une liste d'actions à mettre en œuvre. Le premier axe vise la modernisation de l'administration publique en favorisant l'adoption rapide des TIC. Les autres axes concernent les infrastructures et équipements liés aux TIC, le développement des compétences numériques, l'accès des citoyens au numérique, la promotion de la recherche dans ce domaine et l'adaptation du cadre juridique à l'économie numérique (Refafa.b, 2020) .

Divers exemples illustrent la transition numérique de l'administration publique en Algérie, tels que l'introduction de la carte d'identité, du passeport et du permis de conduire biométriques, la dématérialisation du registre d'état civil facilitant l'obtention de documents administratifs dans la commune de résidence, la mise en place d'un registre national électronique des cartes grises, la possibilité de demander en ligne divers actes administratifs tels que les actes de naissance, de mariage et de décès, avec une extension de leur période de validité. Il convient de noter que de nombreux organismes publics tels que les universités,

les organismes de protection sociale et la justice ont entamé la numérisation de certaines de leurs procédures, en particulier en réponse à la pandémie de la COVID-19.

Les progrès accomplis par l'administration algérienne dans le domaine de la digitalisation sont exposés dans le tableau ci-dessous. En 2020, l'Algérie occupe la 13ème place en Afrique et la 120ème place dans le monde, marquant une amélioration significative par rapport à 2018, bien qu'elle soit devancée par la Tunisie, le Maroc et l'Égypte. Ce classement a été établi en fonction de l'indice de développement de l'e-gouvernance (Refafa.b, 2020) .

Les Nations Unies ont élaboré l'indice de développement de l'e- gouvernance (EGDI) afin de mesurer l'état de préparation et la capacité des institutions nationales à utiliser les TIC pour fournir des services publics. Cet indice composite est basé sur la moyenne pondérée de trois indices normalisés. Un tiers est dérivé l'indice de l'infrastructure des télécommunications, un tiers de l'indice du capital humain et un tiers de l'indice de service en ligne.

En conclusion, ce chapitre a mis en lumière les multiples facettes et enjeux des données personnelles à l'ère du numérique. Sur le plan économique, les données sont devenues une ressource précieuse, alimentant un marché dynamique mais controversé, où la protection de la vie privée et la concurrence économique se confrontent. Politiquement et socialement, les techniques de surveillance soulèvent des préoccupations majeures quant aux libertés individuelles et à l'utilisation des technologies pour le contrôle social. La confidentialité des données, définie comme la protection contre tout accès ou utilisation non autorisée, est encadrée par des régulations telles que le RGPD, visant à instaurer des normes strictes et à garantir les droits des individus. Le cadre juridique en Algérie, bien que récent, marque un progrès significatif vers une meilleure protection des données personnelles, notamment à travers la digitalisation des services publics. Cependant, la mise en œuvre efficace de ces mesures reste un défi crucial pour établir une confiance durable entre les institutions et les citoyens.

Chapitre II : Cadre méthodologique et organisationnel

Après avoir présenté les fondements théoriques sur lesquels s'articule la présente recherche, il serait pertinent de traiter la méthodologie qui encadre notre réflexion et nous guide dans notre travail. Dans ce sens nous avons consacré ce chapitre à la description du cadre méthodologique de l'étude.

L'objet de ce 2ème chapitre est de présenter l'approche méthodologique adoptée en indiquant la posture épistémologique choisie pour bien mener cette étude, ainsi que les techniques de collecte de données utilisées afin d'atteindre les objectifs de cette étude en passons par les outils utilisés dans notre projet d'étude afin d'appuyer l'analyse théorique et justifier l'approche empirique.

II.1 Cadre méthodologique

II.1.1 Positionnement épistémologique

L'utilisation d'une méthode de recherche est souvent la conséquence d'un choix méthodologique et épistémologique. Cohen (1996) définit l'épistémologie comme : *« un simple retour critique de la connaissance sur elle-même, sur son objet, sur ses conditions de formation et de légitimité ; elle est définie comme la philosophie de connaissance, la théorie des sciences ou encore comme la théorie de la connaissance. »*. Jean Piaget de son côté donne une définition plus bref à l'épistémologie *« l'étude de la constitution des connaissances valables »* (Jean, 1967).

L'épistémologie propose de porter un regard sur le statut, la méthode et la valeur de la connaissance en apportant des réponses à trois principales questions :

- Qu'est-ce que la connaissance ?
- Comment est-elle constituée ou engendrée ?
- Comment apprécier sa valeur ou sa validité ?

Chaque chercheur doit déterminer le paradigme épistémologique dans lequel s'inscrit sa recherche, un paradigme désigne *« une constellation de croyances, valeurs, techniques, etc. partagées par une communauté donnée. »* (S. Kuhn, 1962). Pour cela il existe plusieurs paradigmes épistémologiques, les plus connus sont :

- Le positiviste : son fondateur est Auguste Comte qui disait : *« que le mot positif désigne le réel »* (Le Moigne, 1995). Le positiviste a un raisonnement déductif qui veut dire que la véritable connaissance ne peut se fonder sur les sens. La certitude vient de la déduction (de notre raison, de nos raisonnements). A partir des intuitions (ou prémices), il s'agit de déduire d'autres affirmations qui en sont les conséquences (René, 2006).

- Le constructiviste : Largeault disait que : "un objet existe si on est capable de le construire, d'en exhiber un exemplaire ou de le calculer explicitement". Le constructiviste a un raisonnement inductif qui veut dire que l'induction consiste à induire des énoncés généraux (des vérités) à partir d'expériences particulière rigoureuses et systématiques (Largeaut, 1993).

Tableau 1: Les caractéristiques principales des deux paradigmes selon Croom

Positivisme	Constructivisme
• La réalité existe comme vérité • La connaissance est un contexte ouvert • La recherche peut révéler le "vrai" état des affaires • La posture basique est réductionniste et déterministe • La vérification : comment la validité est-elle assurée ?	• La réalité est dépendante à travers l'individuel (existentiel) • La recherche a pour but de regarder le monde à travers le point de vue du sujet. • Pour comprendre, il faut interpréter. • Il est concerné par comment savoir et faire

Source : Croom (1999)

Puisque notre recherche s'inscrit dans le cadre des sciences de gestion, nous nous inscrivons dans une posture épistémologique constructiviste avec un raisonnement inductif.

II.1.2 Approche Méthodologique de la recherche

Le terme « méthode » dans les sciences à un sens très précis, *« Il s'agit de l'ensemble des démarches que suit l'esprit pour découvrir et démontrer la vérité*. La méthodologie étant généralement définie comme : *« l'étude des méthodes destinées à élaborer des connaissances »*, elle apparaît comme l'un des volets de l'épistémologie (Rossi, 2015).

Pour mener à bien notre étude, nous avons opté pour la méthode de recherche qualitative. L'étude qualitative menée par le biais des entretiens semi-directifs a été réalisée le mois d'avril 2024 au niveau de la CNAS Tiaret.

II.1.3 Les outils de collecte des données

La mesure de la qualité d'un service nécessite l'implication de l'acteur central au processus de production du service, à savoir le client. De ce fait l'outil le plus adéquat pour atteindre notre objectif est le questionnaire, car il permet de recueillir une information primaire directement des clients. Afin d'élaboré le questionnaire, nous avons choisi de recueillir des informations sur le sujet à travers la recherche documentaire afin d'obtenir les informations nécessaires et arriver à des résultats fiables et crédibles.

II.1.3.1 La recherche documentaire :

La recherche documentaire permet d'avoir une idée globale sur les différentes théories qui parlent de notre thématique ou qui sont proches de notre sujet de recherche, de définir ou de cadrer notre étude, de construire notre idée à travers des théories et de les combiner pour aboutir au résultat. Les différentes sources documentaires utilisées dans notre travail de recherche sont principalement des ouvrages, des mémoires, des thèses, des articles et des sites web qui sont en relation avec la mesure de la qualité.

II.1.3.2 Entretiens semi-directif :

Selon ANGER.M « Le questionnaire est une technique directe d'investigation scientifique auprès d'individus qui permet de les interroger d'une façon directive et de faire un prélèvement quantitatif » (Anger, 1997). Notre entretien est structuré comme suite :

- **Introduction**

Après avoir accueilli nos interviewés, nous avons commencé par nous présenter et expliquer le but de notre étude. Nous avons souligné que leurs réponses seraient anonymes et confidentielles, puis nous avons exprimé notre gratitude pour leur participation.

- **Les questions d'entretien**

Partie 01 : Présentation de l'interviewé et l'entreprise d'accueille

1. Pouvez-vous nous donner une brève présentation de la Caisse Nationale d'Assurance Sociale (CNAS) et de ses principales missions ?

2. Quel est votre rôle au sein de la CNAS ?

Partie 02 : Les question de l'entretien

Section 1 : Compréhension de la Gouvernance Électronique

3. Comment définiriez-vous la gouvernance électronique ?

4. Pour bien comprendre l'efficacité de la gouvernance électronique au sein de la CNAS, il est essentiel de savoir comment les politiques de gouvernance sont adoptées par la CNAS. Pourriez-vous nous parler du taux d'adoption des politiques de gouvernance au sein de la CNAS et quels sont les principaux défis que vous rencontrez à cet égard ?

5. Avez-vous des statistiques ou des indicateurs précis qui montrent le niveau d'adoption de ces politiques ?

6. Comment la formation continue des employés contribue-t-elle à l'adoption des politiques de gouvernance ?

7. Quel est le niveau de sensibilisation des employés de la CNAS à la gouvernance électronique ?

8. Quels sont les principaux défis que vous rencontrez pour sensibiliser les employés à la gouvernance électronique ?

Section 2 : Confidentialité des Données

9. Comment la CNAS définit-elle la confidentialité des données ?

10. Quelles politiques et procédures spécifiques avez-vous mises en place pour assurer la confidentialité des données ?

11. Quels types de technologies et d'outils utilisez-vous pour protéger la confidentialité des données ?

12. Quel est votre protocole en cas de violation de la confidentialité des données ?

13. Y a-t-il d'autres aspects de la confidentialité des données que vous aimeriez aborder ?

14. Quels sont les principaux défis rencontrés par la CNAS en matière de protection de la confidentialité des données dans le cadre de la gouvernance électronique

Nous avons clôturé les entretiens par des remerciements.

II.1.4 Traitement et analyse des données

Nous allons utiliser l'analyse thématique qualitative pour analyser les réponses recueillies lors de nos entretiens. Cette technique consiste à examiner les propos des répondants en relation avec les thèmes de recherche « *est une méthode d'analyse consistant « à repérer dans des expressions verbales ou textuelles des thèmes généraux récurrents qui apparaissent sous divers contenus plus concrets* » (MUCCHIELLI, 1991)

Nous allons utiliser le logiciel NVivo, qui aide à organiser les données. NVivo permet de coder les réponses, de rechercher des thèmes récurrents, et de visualiser les relations entre les différents éléments des données qualitatives par des nuages de mots. Grâce à ses outils avancés, nous pouvons mieux structurer, analyser et interpréter les informations recueillies, facilitant ainsi une analyse approfondie et rigoureuse de nos entretiens.

II.1.5 Étapes de Traitement des Données d'Entretiens sur NVivo :

Importation des Données : Les entretiens ont été importés en tant qu'éléments internes dans nos sources de données.

Définition des Caractéristiques : Nous avons attribué des caractéristiques spécifiques à chaque entretien, telles que l'identité des participants, la durée des entretiens, et d'autres détails contextuels pertinents. Cette étape organise et structure les données, facilitant une analyse thématique approfondie.

Identification des Thèmes Principaux : Ensuite, nous avons identifié les nœuds, représentant les thèmes principaux des entretiens. Ces nœuds servent de points de référence pour organiser les données en regroupant les informations similaires sous des catégories thématiques.

Encodage des Données : Nous avons ensuite encodé les segments de texte pertinents vers les nœuds correspondants. Chaque segment de phrase ou mot est associé à un thème spécifique, classant ainsi les informations de manière cohérente.

Création de Nuages de Mots : Après l'encodage, nous avons utilisé des nuages de mots pour visualiser graphiquement les termes les plus fréquents ou significatifs associés à chaque thème. Ces visualisations offrent une représentation visuelle intuitive des principaux concepts abordés, aidant à identifier les tendances et les motifs émergents. Les nuages de mots servent également de point de départ pour une analyse plus approfondie, en mettant en lumière les termes clés à explorer davantage.

II.2 Cadre organisationnel

II.2.1 Présentation de l'organisme d'accueil (CNAS Tiaret)

La CNAS est un établissement public à gestion spécifique en application de l'article 49 de la loi n° 88-01 du 12 janvier 1988, elle est dotée de la personnalité morale et de l'autonomie financière, et réputée commerçante dans ses relations avec les tiers.

La Caisse Nationale des Assurances Sociales (CNAS) fournit une couverture à 80% de la population algérienne, ce qui entraîne la génération de données massives. Pour répondre aux exigences de performance, d'efficacité et d'agilité, la CNAS doit structurer de manière adéquate son système d'information et concevoir un système décisionnel approprié.

La CNAS, étant une organisation qui baigne dans un contexte de challenge augmenté vis-à-vis de la qualité des services mettent aux assurés, clientèle de plus en plus exigeante et une réglementation en changement continu, a subi plusieurs évolutions dans son parc Informatique, au fil du temps, dont l'objectif est d'être à jour avec les nouvelles technologies relatives au domaine de l'informatique en plein essor.

Dans le cadre actuel, la CNAS est actuellement confrontée à la nécessité de structurer efficacement son Système d'Information (SI) et de mettre en place un système décisionnel afin d'améliorer ses performances, de fidéliser sa clientèle, tout en prenant en considération son

patrimoine informationnel. La CNAS couvre trois principales catégories de prestations destinées aux assurés sociaux au niveau de chaque centre de paiement, à savoir les prestations en nature, le tiers payant, les prestations en espèces, ainsi que d'autres prestations destinées aux employeurs au niveau de la Caisse Nationale du Recouvrement des Cotisations de la Sécurité Sociale, telles que l'immatriculation, les cotisations, les déclarations des assurés, les abattements, le contrôle des employeurs et le suivi des contentieux.

II.2.1.1 Les missions de la CNAS

La CNAS a pour mission, conformément à la législation en vigueur de :

- Superviser l'attribution des prestations en nature et en espèces des assurances sociales, des accidents du travail et des maladies professionnelles.
- Gérer les allocations familiales.
- Garantir la collecte des cotisations allouées au soutien des avantages sociaux offerts par la CNAS.
- Contribuer à promouvoir la politique de prévention des accidents du travail et des maladies professionnelles, ainsi que gérer les fonds alloués à cette prévention.
- La gestion des prestations destinées aux bénéficiaires des conventions et accords internationaux de sécurité sociale.
- Assurer l'organisation, la coordination et la supervision des activités médicales.
- Entreprendre des actions visant à mettre en œuvre des projets à vocation sanitaire et sociale.
- La mise en œuvre d'actions de prévention, d'éducation et d'information sanitaire est réalisée suite à la recommandation du conseil d'administration de la caisse.
- Gérer le fonds d'aide et de secours.
- Rembourser les frais engagés pour le fonctionnement des différentes commissions ou juridictions chargées de statuer sur les litiges découlant des décisions prises par la caisse.

II.2.1.2 Organisation de la CNAS

La CNAS est administrée par un Conseil d'Administration, elle est placée sous la tutelle du Ministre du travail, de l'Emploi et de la Sécurité Sociale, son siège est à Alger (BEN AKNOUN), elle a compétence nationale et dispose de services centraux et locaux.

II.2.1.3 Les structures de la CNAS

Pour remplir ses missions, la CNAS dispose de :

- Une Direction générale
- 49 Agences de wilaya (dont 2 à Alger)
- 826 structures de paiement, dont :
- 356 centres de paiement
- 401 antennes de paiement
- 69 correspondances locales.
- 4 cliniques spécialisées (chirurgie cardiaque infantile, orthopédie et rééducation, ORL, dentaire)
- 4 centres régionaux d'imagerie médicale
- 35 centres de diagnostic et de soins
- 55 officines pharmaceutiques
- 30 crèches et jardins d'enfant ;
- Une imprimerie à Constantine ;
- Un centre familial à caractère social à Ben Aknoun.

II.2.1.4 Les bénéficiaires

- Les travailleurs salariés, quel que soit le secteur d'activité ;
- Les apprentis ;
- Les bénéficiaires des emplois d'attente ;
- Les étudiants
- Les stagiaires de la formation professionnelle

- Les handicapés
- Les moudjahidines (anciens combattants)
- Les titulaires d'avantages de sécurité sociale (pensionnés et rentiers)
- Les bénéficiaires de l'allocation forfaitaire de solidarité (personnes malades ou âgées et inactives) Il faut ajouter les ayants droit qui sont :
    - Le conjoint.
    - Les enfants mineurs.
    - Les filles inactives non mariées.
    - Les ascendants à charge.

II.2.1.5 Les prestations

- Les soins de santé et les médicaments sont pris en charge à 80 % et dans certains cas à 100% (malades chroniques notamment) ;
- L'indemnisation des arrêts de travail pour maladie représente 50 % du salaire pendant les 15 premiers jours. Elle est portée à 100 % du salaire au-delà du 16ème jour ;
- La durée maximale de cette indemnisation est de trois ans ;
- Les prestations de l'assurance maternité sont prises en charge à 100 %, la femme travailleuse bénéficie d'un congé de maternité de 98 jours ;
- Le montant minimum des pensions d'invalidité est égal à 75 % du SNMG ;
- Au décès de l'assuré, il est servi un capital décès à ses ayants droit ;
- Les risques professionnels donnent lieu à une couverture à 100 % pour les soins et les arrêts de travail ;
- Des rentes sont versées en cas de séquelles corporelles de l'accident ;
- Des rentes sont servies aux ayants droit en cas d'accident mortel.

II.2.2 Les systèmes d'information développés par la CNAS

Le Système intégré de gestion des assurés sociaux (SIGAS) gère les demandes de prestations en prenant en charge les compensations journalières lorsque l'assuré est en arrêt de travail en

raison de maladie, de maternité, d'accident du travail, de maladie professionnelle, d'invalidité, de décès ou pour les allocations familiales.

Actuellement, le système en place repose sur une architecture Client-Serveur, impliquant la Direction Informatique, les agences et les entités de paiement. Des serveurs de bases de données relationnelles sont déployés au sein de la Direction Informatique.

Le système SECU est responsable de la gestion de l'immatriculation, des cotisations de sécurité sociale et du recouvrement comptable. Autres systèmes d'information qui fait partie du parc informatique du CNAS est :

- Le système intégré de gestion du contrôle médical (SIGCM) utilisé par les médecins-conseils facilite la prise de décision concernant les diverses prestations (maladie, maternité, accident de travail...).

- Le système intégré de gestion des appareillages permet la gestion et le contrôle de la distribution des appareillages aux assurés sociaux ayant des besoins particuliers. Le logiciel DAS est chargé de la gestion des déclarations annuelles des assurés sociaux et des cotisations des employeurs.

- Le logiciel Emploi est chargé de la gestion des réductions de cotisations dont bénéficient les employeurs participant au dispositif d'encouragement à l'emploi.

- Le logiciel de comptabilité.

- Le logiciel de gestion des ressources humaines.

- Le logiciel de gestion des stocks et de l'inventaire physique.

- Le système de gestion de la documentation électronique.

- Un système de registration pour la carte CHIFA.

II.2.3 La gouvernance électronique de la CNAS Algérie

Ces dernières années, l'Algérie a introduit des systèmes électroniques dans le secteur public dans le but de développer les prestations en ligne, d'améliorer les services de secteur pour les

citoyens et de diffuser la transparence grâce à des systèmes avancés.

Dans ce contexte, l'Algérie, comme de nombreux pays, a œuvré au développement et à la promotion du secteur.

La Sécurité Sociale, ainsi que les programmes de développement et de modernisation suivis par le Ministère, qui est le gardien du secteur, ont donné naissance à un nouveau mécanisme de protection et d'assurance sociale en Algérie et même en Afrique, qui est une carte électronique appelée « Carte de chiffa » (Refafa.b, 2020)

L'évolution de ce mécanisme s'est déroulée de manière progressive en suivant une stratégie bien définie, et a bénéficié de l'implication des compétences nationales du domaine de la sécurité sociale en Algérie. Le processus a été initié entre avril et juillet 2007 avec l'ouverture d'un centre de personnalisation des premières cartes, ainsi que la réception des premières factures électroniques des pharmaciens. En 2009, ces cartes ont été distribuées et l'utilisation de la carte Chiffa a débuté avec le médecin traitant, puis s'est étendue aux fabricants de dispositifs médicaux. En août 2011, l'utilisation de la carte a été généralisée à l'ensemble du territoire national.

La CNAS, en tant que Caisse Nationale d'Assurance Sociale, gère un grand nombre de données sensibles sur ses assurés, y compris des informations médicales, financières et personnelles. La confidentialité de ces données est d'une importance capitale pour protéger les assurés contre le vol, l'abus et la discrimination (Refafa.b, 2020)

En 2020, la CNAS a subi une cyberattaque qui a eu un impact majeur sur la confidentialité des données de ses assurés. Cette attaque a mis en lumière la vulnérabilité des systèmes informatiques de la CNAS et a soulevé des inquiétudes concernant la protection des données sensibles des citoyens algériens (Refafa.b, 2020) Effectivement, en 2020, la CNAS a subi une cyberattaque qui a eu un impact majeur sur la confidentialité des données de ses assurés. Cette attaque a mis en lumière la vulnérabilité des systèmes informatiques de la CNAS et a soulevé des inquiétudes concernant la protection des données La numérisation des services de la CNAS

La caisse nationale des assurances sociales des travailleurs salariés (CNAS) gère le recouvrement de toutes les cotisations sociales pour son compte et le compte des autres caisses : caisse nationale des retraites CNR, caisse nationale d'assurance chômage CNAC et fonds national de péréquation des œuvres sociales FNPOS. Elle assure aussi le paiement des

prestations et gère les prestations relatives aux accidents de travail et les maladies professionnelles ainsi que celles liées aux bénéficiaires des conventions internationales de sécurité sociale. Par ailleurs, elle organise le contrôle médical et gère les prestations familiales.

II.2.3.1 Les services numériques proposés par la CNAS

Afin de moderniser les prestations de la CNAS et faciliter les procédures administratives en faveur des assurés sociaux notamment les personnes âgées et les personnes aux besoins spécifiques, des efforts de modernisation des services publics ont été consenti par cet organisme. Pour ce faire, plusieurs espaces ont été créés, en l'occurrence El Hana, télé-déclaration, carte CHIFA, e-paiement.

- **Espace El Hanaa**

Lancé en 2016, l'espace El Hanaa est une plateforme en ligne qui offre aux assurés sociaux la possibilité de générer leurs attestations d'affiliation, leurs certificats d'éligibilité aux prestations, de suivre l'avancement de leurs demandes de remboursement de médicaments et de recevoir les convocations pour les contrôles médicaux. De plus, les assurés peuvent signaler leurs arrêts de travail via cette plateforme, en téléchargeant électroniquement un certificat d'arrêt de travail et en suivant les démarches pour déclarer un congé maladie. Les autorités publiques, quant à elles, peuvent vérifier la validité des attestations d'affiliation sur l'espace El Hanaa.

- **Télédéclaration**

La télédéclaration concerne la déclaration de l'assiette de cotisation (DAC), au cours de laquelle l'employeur spécifie la rémunération et les cotisations à verser pour chaque salarié, que ce soit sur une base mensuelle ou trimestrielle. En ce qui concerne la déclaration annuelle des salaires et des salariés (DAS), elle récapitule l'ensemble des DAC effectuées au cours d'une année. Les employeurs ont également la possibilité de consulter la situation de leurs employés et de soumettre des demandes d'affiliation pour de nouveaux salariés, notamment les ressortissants algériens sensibles (Refafa.b, 2020).

- **E-paiement**

Depuis 2020, on observe une augmentation significative du paiement en ligne en Algérie. Selon les données du GIE Monétique, le volume des transactions en ligne a été multiplié par plus de trois en 2022 par rapport à 2020, avec plus de 9 millions de transactions enregistrées d'ici le 31 décembre 2022. La CNAS a également suivi cette tendance depuis 2016 en proposant aux

employeurs la possibilité de régler leurs cotisations en ligne, que ce soit par carte interbancaire ou via des terminaux de paiement électronique installés dans les locaux de la CNAS. Initialement limitée aux clients de la Banque de Développement Local (BDL), la digitalisation du paiement des cotisations sociales s'est ensuite étendue à l'ensemble des cartes de paiement disponibles.

- **La télé-demande**

Elle permet d'envoyer en ligne la demande d'immatriculation et d'affiliation des assurés sociaux comme elle permet aux employeurs de demander en ligne la carte « Chiffa » des employés.

- **Le système Chiffa**

Ce mécanisme repose sur l'utilisation de la carte Chiffa, facilitant ainsi un remboursement rapide en simplifiant les procédures administratives et en renforçant l'interaction entre les patients, les médecins et les pharmaciens. De plus, la traçabilité offerte par cette carte contribue à la lutte contre les fraudes abusives. Les données contenues dans cette carte concernent les droits aux prestations, les accords contractuels, les actes remboursés ainsi que d'autres informations techniques.

Le déploiement du projet "système Chiffa" a été initié en 2004, mais sa généralisation à l'ensemble des agences CNAS n'a été achevée qu'en 2010. En 2011, une extension du système du tiers-payant pour les produits pharmaceutiques à tous les bénéficiaires de la carte Chiffa a été mise en place, suivie en 2013 par l'expansion de l'utilisation de la carte Chiffa à l'échelle nationale. Le pharmacien, acteur clé de ce dispositif, réalise plusieurs vérifications telles que la validation de la carte, le suivi des consommations de médicaments et la création de la facture électronique qu'il transmet ensuite à la CNAS.

- **« AraaCom » أراءكم**

C'est une plateforme qui permet aux citoyens de s'exprimer sur leurs préoccupations en formulant des propositions permettant d'améliorer le service rendu par la CNAS. Elle est disponible via le lien « Araacom ministère, « partagez vos propositions ».

II.2.4 Etat de système de sécurité de la CNAS

Les menaces potentielles des cyber-attaques contre les technologies de l'information et de la communication ont provoqué des pertes économiques et un climat d'insécurité et d'incertitude envers les services numériques. Ceci appelle à appliquer des contremesures qui protègent les organismes et les infrastructures critiques, préservent les intérêts vitaux du pays et renforcent la sécurité nationale. La CNAS a connu un cyber attaque en octobre 2020, les détails de cette attaque est présenté dans le tableau suivant.

Tableau 2: Quelques détails importants concernant cette cyberattaque sur la CNAS

Date	Octobre 2020.
Nature de l'attaque	Ransomware (rançongiciel). (Annexe C)
Impact	Exfiltration de données sensibles de millions d'assurés, y compris des informations médicales, financières et personnelles.
Conséquences	Perturbation des services de la CNAS, inquiétudes et méfiance des assurés.

Source : CNAS Algérie, 2024

Suite à cette attaque, la CNAS a pris plusieurs mesures pour renforcer la sécurité de ses systèmes informatiques et protéger les données de ses assurés :

- ✓ Mise en place d'un nouveau système de sécurité informatique.
- ✓ Renforcement des contrôles d'accès aux données.
- ✓ Sensibilisation des employés aux risques de cyberattaques.
- ✓ Collaboration avec les autorités pour identifier les auteurs de l'attaque.

Malgré ces efforts, l'attaque de 2020 a eu un impact durable sur la CNAS et sur la confiance des citoyens algériens dans les services publics en ligne. Il est important que la CNAS continue à investir dans la sécurité de ses systèmes informatiques et à mettre en place des mesures de protection des données robustes pour garantir la confidentialité des informations sensibles de ses assurés.

En conclusion, ce chapitre a exposé le cadre méthodologique essentiel pour notre recherche, détaillant l'approche méthodologique adoptée, la posture épistémologique choisie, ainsi que les techniques de collecte de données employées. En décrivant minutieusement les outils utilisés pour soutenir notre analyse théorique et justifier notre approche empirique, nous avons mis en lumière les éléments clés qui guideront notre investigation et nous permettront d'atteindre les objectifs de cette étude. Cette méthodologie rigoureuse constitue donc la base solide sur laquelle reposera l'ensemble de notre travail de recherche**.** Ainsi, nous avons exposé l'entreprise d'accueille la CNAS unité de Tiaret et ces services, et un état de lieu approfondie du notre sujet de recherche dans cet établissement.

Chapitre III : Présentation et discussion des résultats

Cette section décrit la partie pratique de notre recherche. Elle commence par la présentation des résultats qualitatifs obtenus, se poursuit par une analyse approfondie de ces résultats, et se termine par des suggestions éclairées.

III.1 Présentation des résultats

Tout d'abord, nous présenterons les données recueillies à partir des entretiens semi-directifs réalisés avec 04 participants. Ensuite, nous procéderons à leur analyse.

III.1.1 Présentation de participants interviewé

Pour collecter les données nécessaires à notre étude, nous avons mené des entretiens avec quatre dirigeants de l'entreprise d'accueil, CNAS. Le tableau ci-dessous résume les informations professionnelles de ces participants ainsi que la durée de chaque entretien.

Tableau 3: Attribue des interviewés

Interviwés	Fonction occupée	Sexe	Durée d'entretien
I1	Directeur de la CNAS	Homme	31 mins
I2	Directeur RH de la CNAS	Homme	20 mins
I3	Chef Bureau s/d informatique	Homme	20 mins
I4	Chef de projet Intelligence d'affaires	Homme	40 mins

Source : élaboré par nos soins

III.1.2 Traitement et analyse des résultats

III.1.2.1 Compréhension de la Gouvernance Électronique

I01	*« La gouvernance électronique peut être définie comme l'intégration des technologies pour améliorer la prestation des services publics, visant à optimiser l'efficacité, la transparence et la responsabilité. »*
I02	*« La gouvernance électronique se définit par l'utilisation de l'informatique pour améliorer les processus administratifs, les services publics et l'interaction entre le gouvernement et les citoyens. »*
I03	*« Par la numérisation. »*
I04	*« La gouvernance électronique vise à exploiter le potentiel des technologies de l'information et de la communication pour promouvoir une gouvernance plus efficace, transparente, inclusive et responsable, tout en offrant des services publics de meilleure qualité et en répondant aux besoins et aux attentes des citoyens dans un environnement numérique »*

Les extraits de verbatim ci-dessous proviennent des réponses des interviewé aux question 3

La majorité des interviewés, I1, I2 et I4, ont défini la gouvernance électronique comme l'intégration des technologies pour améliorer la prestation des services publics, visant à optimiser l'efficacité, la transparence et la responsabilité. I1 met l'accent sur ces objectifs clés, tandis que I2 ajoute l'amélioration des processus administratifs et l'interaction entre le gouvernement et les citoyens. I4 élargit encore cette définition en incluant les notions d'inclusivité et de promotion d'une gouvernance plus responsable, tout en offrant des services publics de meilleure qualité et en répondant aux besoins des citoyens dans un environnement numérique. À l'inverse, I3 fournit une définition plus succincte, se contentant de mentionner la numérisation sans détailler les aspects spécifiques de la gouvernance électronique. En somme, bien que tous les interviewés reconnaissent l'importance des technologies dans la gouvernance électronique, la majorité souligne l'optimisation de l'efficacité, la transparence et la

responsabilité, avec des ajouts significatifs de certains sur l'inclusivité et la qualité des services publics.

Les extraits de verbatim ci-dessous proviennent des réponses des interviewé aux question 4

I01	*« Aucune réponse. »*
I02	*« À la CNAS, l'adoption des politiques de gouvernance électronique suit un processus structuré. Les politiques sont élaborées en consultation avec divers départements pour assurer qu'elles répondent aux besoins spécifiques de chaque secteur. »*
I03	*« Les politiques de gouvernance électronique sont développées, approuvées et mises en œuvre au sein de la CNAS, par l'intégration des opérations quotidiennes de la CNAS »*
I04	*« Les politiques de gouvernance électronique sont non seulement conformes aux exigences légales et réglementaires, mais aussi adaptées aux besoins spécifiques de la CNAS, contribuant ainsi à une meilleure protection des données et à une efficacité accrue des services »*

La majorité des interviewés, I2, I3 et I4, ont décrit l'adoption des politiques de gouvernance électronique à la CNAS comme un processus structuré et intégré, visant à répondre aux besoins spécifiques de l'organisation. I2 met en avant l'élaboration des politiques en consultation avec divers départements pour assurer leur pertinence sectorielle. I3 souligne que les politiques sont développées, approuvées et mises en œuvre en intégrant les opérations quotidiennes de la CNAS, ce qui garantit leur applicabilité pratique. I4 ajoute que ces politiques sont conformes aux exigences légales et réglementaires et sont adaptées aux besoins spécifiques de la CNAS, contribuant ainsi à une meilleure protection des données et à une efficacité accrue des services. À l'inverse, I1 n'a pas fourni de réponse, ce qui peut indiquer une absence de connaissance ou d'opinion sur le sujet. En somme, bien que les réponses varient en détail, la majorité des interviewés souligne une adoption structurée et intégrée des politiques de gouvernance électronique, avec un accent sur la conformité, l'adaptabilité et l'efficacité opérationnelle.

Les extraits de verbatim ci-dessous proviennent des réponses des interviewés aux question 5

I01	*« Le taux d'adoption des politiques de gouvernance au sein de la CNAS Tiaret est actuellement estimé à environ 85%. Cependant, des défis tels que la résistance au changement chez certains employés et le besoin constant de mise à jour des compétences en raison de l'évolution rapide des technologies sont rencontrés »*
I02	*« Le taux d'adoption des politiques de gouvernance électronique au sein de la CNAS est généralement élevé. Nous estimons que plus de 90% de nos employés appliquent régulièrement les politiques mises en place »*
I03	*« Je n'ai pas d'informations de ce type »*
I04	« Le taux d'adoption des politiques de gouvernance au sein de la CNAS est généralement élevé, mais de préférence voir avec les responsables de la CNAS »

La majorité des interviewés, I1, I2 et I4, ont décrit le taux d'adoption des politiques de gouvernance électronique au sein de la CNAS comme étant élevé. I1 estime ce taux à environ 85% à la CNAS Tiaret, mais mentionne des défis comme la résistance au changement chez certains employés et la nécessité de mises à jour régulières des compétences en raison de l'évolution rapide des technologies. I2 indique que plus de 90% des employés appliquent régulièrement les politiques mises en place, soulignant ainsi un taux d'adoption encore plus élevé. I4 confirme que le taux d'adoption est généralement élevé, mais suggère de consulter les responsables de la CNAS pour des informations plus précises. À l'inverse, I3 n'a pas fourni d'informations spécifiques sur le taux d'adoption, ce qui peut indiquer un manque de connaissance ou d'accès à ces données. En somme, bien que les taux estimés varient légèrement, la majorité des interviewés s'accordent sur une adoption élevée des politiques de gouvernance électronique, tout en soulignant des défis liés à la gestion du changement et à la formation continue des employés.

Les extraits de verbatim ci-dessous proviennent des réponses des interviewés aux question 6

I01	*« Oui, plusieurs indicateurs clés sont suivis, tels que le taux de participation aux formations sur la gouvernance, le nombre d'incidents de sécurité signalés et résolus, ainsi que les résultats des audits de conformité. Par exemple, la dernière formation sur la sécurité des données a vu une participation de 90% des employés »*
I02	*« Je n'ai pas des données »*
I03	*« Je n'ai pas d'informations de ce type »*
I04	« Non »

La majorité des interviewés, I1, I2 et I3, ont fourni des réponses variées sur les statistiques ou indicateurs précis montrant le niveau d'adoption des politiques de gouvernance électronique. I1 indique que plusieurs indicateurs clés sont suivis, tels que le taux de participation aux formations sur la gouvernance, le nombre d'incidents de sécurité signalés et résolus, ainsi que les résultats des audits de conformité. Par exemple, la dernière formation sur la sécurité des données a vu une participation de 90% des employés, montrant ainsi un engagement significatif. À l'inverse, I2 et I3 n'ont pas fourni de données spécifiques, signalant un manque de connaissance ou d'accès à ces informations. I4, quant à lui, a répondu négativement, indiquant l'absence de statistiques ou d'indicateurs précis. En somme, bien que I1 fournisse des détails sur les indicateurs suivis, la majorité des interviewés manquent de données spécifiques ou n'ont pas accès à des informations précises sur le niveau d'adoption des politiques de gouvernance électronique.

Les extraits de verbatim ci-dessous proviennent des réponses des interviewés aux question 7

I01	*« La formation continue est cruciale pour maintenir un haut niveau de conformité. Des sessions de formation régulières et des ateliers sont organisés pour que tous les employés soient au courant des dernières politiques et des meilleures pratiques. Ces formations sont obligatoires et incluent des évaluations pour garantir que les informations sont bien assimilées »*

I02	*« La formation continue des employés joue un rôle crucial dans l'adoption réussie des politiques de gouvernance électronique au sein de la CNAS. Nous avons toujours un plan de formation à suivre dans ce cadre. »*
I03	*« Bien que la formation ait un impact sur l'adoption des politiques de gouvernance au sein de la CNAS. »*
I04	*« La formation continue permet aux employés de se tenir au courant des dernières évolutions technologiques, des nouvelles pratiques de gouvernance et des réglementations. Elle permet de développer des compétences spécifiques, telles que la gestion des données et la sécurité informatique. »*

La formation continue des employés joue un rôle crucial dans l'adoption des politiques de gouvernance électronique au sein de la CNAS, selon les réponses des interviewés. I1 souligne l'importance des sessions de formation régulières et des ateliers obligatoires pour maintenir un haut niveau de conformité. Ces formations sont conçues pour informer les employés des dernières politiques et des meilleures pratiques, avec des évaluations pour garantir l'assimilation des informations. De même, I2 mentionne l'existence d'un plan de formation continu pour soutenir l'adoption réussie des politiques de gouvernance électronique. I4 souligne que la formation continue permet aux employés de rester à jour sur les évolutions technologiques, les pratiques de gouvernance et les réglementations, en développant des compétences spécifiques telles que la gestion des données et la sécurité informatique. En revanche, la réponse de I3 est plus concise et n'approfondit pas spécifiquement le lien entre la formation continue et l'adoption des politiques de gouvernance. En résumé, la formation continue est considérée comme un pilier essentiel pour favoriser l'adoption et la conformité aux politiques de gouvernance électronique, en fournissant aux employés les connaissances et compétences nécessaires pour les mettre en œuvre efficacement.

Les extraits de verbatim ci-dessous proviennent des réponses des interviewés aux question 8

I01	*« Le niveau de sensibilisation des employés à la gouvernance électronique est assez élevé, surtout grâce aux programmes de formation réguliers qui ont été mis en place »*
I02	*« Globalement, nous avons mis en place des initiatives de sensibilisation pour garantir que nos employés comprennent pleinement les enjeux liés à la gouvernance électronique et leur rôle dans la protection des données de nos assurés »*
I03	*« Je m'excuse, mais je ne suis pas en mesure de fournir une réponse directe à votre question sans l'input d'un représentant de la CNAS. Le niveau de sensibilisation des employés à la gouvernance électronique peut varier en fonction de nombreux facteurs, tels que les initiatives de formation en place, la communication interne, et la culture organisationnelle. Pour obtenir une réponse précise, il serait préférable de consulter le responsable de la CNAS qui serait en mesure de fournir des informations basées sur des données concrètes et une expérience directe au sein de la CNAS. »*
I04	*« Voir la CNAS je n'ai pas d'information. »*

En ce qui concerne le niveau de sensibilisation des employés à la gouvernance électronique au sein de la CNAS, les réponses des interviewés varient. I1 rapporte un niveau de sensibilisation assez élevé, attribuable en grande partie aux programmes de formation réguliers mis en place. De même, I2 souligne les initiatives de sensibilisation visant à garantir une compréhension complète des enjeux liés à la gouvernance électronique et du rôle des employés dans la protection des données. Cependant, I3 s'excuse de ne pas pouvoir fournir une réponse directe, mentionnant que le niveau de sensibilisation peut varier en fonction de facteurs tels que les initiatives de formation, la communication interne et la culture organisationnelle, suggérant de consulter un représentant de la CNAS pour des informations basées sur des données concrètes. I4 renvoie également à la CNAS pour des informations, indiquant un manque d'informations spécifiques sur le sujet. En résumé, bien que certaines réponses témoignent d'un niveau de sensibilisation élevé grâce aux initiatives de formation, d'autres suggèrent un besoin potentiel d'évaluation plus approfondie pour obtenir une réponse précise sur le niveau de sensibilisation des employés à la gouvernance électronique.

Les extraits de verbatim ci-dessous proviennent des réponses des interviewés aux question 9

I01	*« Le principal défi est la résistance au changement, en particulier chez les employés qui sont avec nous depuis longtemps et qui ont des habitudes bien ancrées. Pour surmonter cela, des efforts de communication ont été intensifiés et des exemples concrets de violations de données sont utilisés pour illustrer les risques et l'importance de la conformité. »*
I02	« Plusieurs défis sont rencontrés, les principaux étant la complexité des sujets et le changement de culture. »
I03	*« Je m'excuse, mais je ne suis pas en mesure de fournir une réponse directe à votre question sans l'input d'un représentant de la CNAS. »*
I04	*« Voir la CNAS je n'ai pas d'information. »*

Lorsqu'il s'agit des principaux défis rencontrés pour sensibiliser les employés à la gouvernance électronique, les réponses des interviewés reflètent une variété de perspectives. Selon I1, la résistance au changement constitue le principal défi, en particulier chez les employés ayant des habitudes bien ancrées. Pour y faire face, des efforts de communication ont été intensifiés et des exemples concrets de violations de données sont utilisés pour illustrer les risques et l'importance de la conformité. I2 souligne également plusieurs défis, notamment la complexité des sujets et le changement de culture. En revanche, I3 et I4 s'excusent de ne pas pouvoir fournir de réponse directe ou d'informations sur les défis spécifiques rencontrés pour sensibiliser les employés à la gouvernance électronique, renvoyant à la CNAS pour de telles informations. En résumé, les principaux défis identifiés incluent la résistance au changement, la complexité des sujets et le changement de culture, avec une reconnaissance générale de la nécessité de renforcer la communication et de fournir des exemples concrets pour sensibiliser efficacement les employés.

Figure 5: Nuage de mots correspondant à la compréhension du Gouvernance Électronique

Source : élaboré par nos soins

Selon le nuage de mots généré à partir l'analyse des entretiens, les termes les plus fréquemment évoqués par les participants incluent principalement la sécurité, la formation, les indicateurs, les technologies, la responsabilité, les services, la conformité, l'amélioration, la résistance, et la protection, entre autres.

III.1.2.2 Confidentialité des Données (sensibilisation et défis)

Les extraits de verbatim ci-dessous proviennent des réponses des interviewés aux question 10

I01	*« La confidentialité des données est définie comme la protection des informations sensibles de nos assurés contre tout accès non autorisé, divulgation, altération ou destruction. »*
I02	*« À la CNAS, nous définissons la confidentialité des données comme la protection et la préservation de l'intégrité »*

I03	*« Nous garantissons que seules les personnes autorisées ont accès aux données sensibles, en mettant en place des contrôles d'accès et des mesures de sécurité appropriées pour protéger les informations contre tout accès non autorisé »*
I04	*« La confidentialité des données est définie comme la protection des informations personnelles et sensibles des assurés et des autres parties prenantes contre les accès non autorisés, les altérations et les divulgations. Cela inclut la mise en place de mesures de sécurité strictes pour protéger les données, la restriction de l'accès aux seules personnes autorisées, la conformité avec les lois et réglementations sur la protection des données, et la garantie de l'intégrité et de l'exactitude des informations »*

La définition de la confidentialité des données à la CNAS varie légèrement selon les réponses des interviewés. Selon I1, il s'agit de la protection des informations sensibles des assurés contre tout accès non autorisé, divulgation, altération ou destruction. I2 la décrit comme la protection et la préservation de l'intégrité des données. I3 souligne l'importance de limiter l'accès aux seules personnes autorisées par le biais de contrôles d'accès et de mesures de sécurité appropriées. I4 élargit cette définition en incluant la protection des informations personnelles et sensibles des assurés et autres parties prenantes contre tout accès non autorisé, altération et divulgation, en mettant en place des mesures de sécurité strictes, en restreignant l'accès aux personnes autorisées, en se conformant aux lois et réglementations sur la protection des données, et en garantissant l'intégrité et l'exactitude des informations. En résumé, la CNAS définit la confidentialité des données comme la protection et la préservation des informations sensibles, avec un accent sur la limitation de l'accès et le respect des lois et réglementations sur la protection des données.

Les extraits de verbatim ci-dessous proviennent des réponses des interviewés aux question 11

I01	*« Nous avons mis en place une série de politiques et procédures. Pour plus d'informations, voir avec la sous-direction Informatique »*

I02	*« Nous avons mis en place plusieurs politiques et procédures spécifiques pour garantir la confidentialité des données de nos assurés. Voir avec la sous-direction Informatique »*
I03	*« Gestion des Accès, Sécurité des Informations, Gestion des Incidents, Formation et Sensibilisation »*
I04	*« Afin d'assurer la confidentialité des données au sein de la CNAS, nous avons mis en place plusieurs politiques et procédures spécifiques, dont voici quelques exemples :* • *Définit les principes et obligations en matière de protection des informations personnelles.* • *Contrôle d'Accès pour limiter l'accès aux données sensibles aux seules personnes autorisées.* • *Utilisation du chiffrement pour protéger les informations sensibles pendant leur transmission et leur stockage.* • *Système centralisé pour gérer les identités des utilisateurs et leurs droits d'accès.* *Audits réguliers des systèmes et des données pour identifier les vulnérabilités et les activités suspectes »*

Pour garantir la confidentialité des données, la CNAS a mis en place diverses politiques et procédures. Selon les interviewés : I1 et I2 renvoient à la sous-direction Informatique pour obtenir plus d'informations sur ces politiques. I3 énumère plusieurs domaines de gestion, notamment la Gestion des Accès, la Sécurité des Informations, la Gestion des Incidents et la Formation et Sensibilisation. I4 fournit des exemples spécifiques, tels que des politiques sur la protection des informations personnelles, le contrôle d'accès restreint, l'utilisation du chiffrement pour sécuriser les données, un système centralisé pour gérer les identités et les droits d'accès, ainsi que des audits réguliers des systèmes et des données pour identifier les vulnérabilités et les activités suspectes. En résumé, pour assurer la confidentialité des données, la CNAS a mis en place des politiques et procédures spécifiques couvrant divers aspects de la gestion des données sensibles.

Les extraits de verbatim ci-dessous proviennent des réponses des interviewés aux question 12

I01	*« Nous utilisons des solutions de chiffrement avancées. Pour plus d'informations, voir avec la sous-direction Informatique. »*
I02	*« Nous utilisons une gamme de technologies et d'outils pour garantir la protection de la confidentialité des données de nos assurés. Voir avec la sous-direction Informatique. »*
I03	*« Nous utilisons des techniques de cryptage pour sécuriser les données sensibles lorsqu'elles sont stockées, en transit ou en cours d'utilisation. Contrôles d'Accès et d'Identification »*
I04	*« Nous avons utilisé une gamme de technologies et d'outils pour protéger la confidentialité des données, notamment :* • *Chiffrement des données pour sécuriser les données lors de leur transmission et de leur stockage.* • *Pare-feu et sécurité des réseaux pour prévenir les intrusions et les attaques extérieures.* • *Gestion des identités et des accès pour contrôler les accès aux systèmes et aux données.* • *Systèmes de détection des menaces pour détecter les activités suspectes et les comportements anormaux.* *Gestion des vulnérabilités pour identifier et corriger les failles de sécurité »*

Les réponses des interviewés démontrent une utilisation variée de technologies et d'outils pour assurer la protection de la confidentialité des données au sein de la CNAS. I1 et I2 renvoient à la sous-direction Informatique pour obtenir plus de détails sur les solutions de chiffrement avancées et les technologies utilisées. I3 mentionne spécifiquement l'utilisation de techniques de cryptage pour sécuriser les données sensibles lorsqu'elles sont stockées, en transit ou en cours d'utilisation, ainsi que des contrôles d'accès et d'identification. I4 fournit une liste détaillée des technologies et outils utilisés, comprenant le chiffrement des données, les pares-feux et la sécurité des réseaux, la gestion des identités et des accès, les systèmes de détection des menaces, et la gestion des vulnérabilités.

Les extraits de verbatim ci-dessous proviennent des réponses des interviewés aux question 13

I01	*« En cas de violation de la confidentialité des données, nous avons un protocole strict. Pour plus d'informations, voir avec la sous-direction Informatique. »*
I02	*« Notre protocole en cas de violation de la confidentialité des données à la CNAS est conçu pour garantir une réponse rapide, efficace et coordonnée pour minimiser les impacts sur nos assurés et protéger leurs informations sensibles. Voir avec la sous-direction Informatique. »*
I03	*« Voici les étapes principales de notre protocole : Détection et Signalement, Évaluation Initiale, Gestion de l'Incident »*
I04	*« Le protocole en cas de violation de la confidentialité des données à la CNAS est structuré pour une réponse rapide et coordonnée :* • *Dès la détection d'une violation, une enquête est lancée pour en comprendre l'étendue.* • *Les systèmes affectés sont isolés pour limiter la propagation de la violation.* • *L'évaluation de l'étendue des dommages comprend la détermination des données compromises et des individus impactés.* • *Notifier les autorités compétentes et les parties prenantes sont notifiées conformément aux réglementations en vigueur.* • *Informer les assurés et autres parties prenantes de la violation et des mesures prises pour y remédier.* • *Analyse post-incident pour identifier les causes et les leçons à tirer de l'incident.* • *Un suivi est assuré pour garantir la mise en œuvre des mesures correctives et la production de rapports complets. »*

Les réponses des interviewés décrivent un protocole rigoureux en cas de violation de la confidentialité des données à la CNAS. I1 et I2 renvoient à la sous-direction Informatique pour obtenir plus d'informations sur ce protocole, soulignant ainsi son importance. I3 énumère les étapes principales du protocole, incluant la détection et le signalement, ainsi que l'évaluation

initiale et la gestion de l'incident. I4 détaille un protocole structuré comprenant plusieurs étapes : dès la détection d'une violation, une enquête est lancée pour en comprendre l'étendue, les systèmes affectés sont isolés, une évaluation des dommages est réalisée, les autorités compétentes sont informées, les assurés et autres parties prenantes sont notifiés, une analyse post-incident est effectuée pour tirer des leçons, et un suivi est assuré pour garantir la mise en œuvre des mesures correctives.

Les extraits de verbatim ci-dessous proviennent des réponses des interviewés aux question 14

I01	*« Je tiens à souligner que la confidentialité des données est une responsabilité collective au sein de la CNAS. Nous nous efforçons de créer une culture organisationnelle où chaque employé comprend l'importance de protéger les informations sensibles et s'engage activement à respecter les politiques de confidentialité »*
I02	*« Voir avec la sous-direction Informatique »*
I03	*« En plus des mesures de sécurité numériques, il faut des mesures de sécurité physiques pour protéger les données sensibles. La sensibilisation des assurés »*
I04	**«** Pour le moment, non **»**

La majorité des interviewés, dont I1, soulignent l'importance de créer une culture organisationnelle où chaque employé comprend et s'engage activement à respecter les politiques de confidentialité. Cependant, une partie des répondants, comme I2, renvoie à la sous-direction Informatique pour plus de détails, suggérant un aspect technique supplémentaire à explorer. D'autres, comme I3, évoquent également la nécessité de prendre en compte des mesures de sécurité physiques en plus des mesures numériques, mettant en avant l'importance de sensibiliser également les assurés. En revanche, une réponse négative est donnée par I4, indiquant qu'il n'y a pas d'autres aspects de la confidentialité des données à aborder pour le moment.

Les extraits de verbatim ci-dessous proviennent des réponses des interviewés aux question 15

I01	*« La CNAS rencontre plusieurs défis majeurs en matière de protection de la confidentialité des données dans le cadre de la gouvernance électronique. Ces défis incluent la gestion des accès et des autorisations, la protection contre les cybermenaces, ainsi que la sensibilisation et la formation continue du personnel »*
I02	*« C'est purement technique. Voir avec la sous-direction Informatique. »*
I03	*« L'évolution des Menaces de Sécurité, la complexité des Systèmes d'Information »*
I04	*« La gestion des données électroniques devient de plus en plus complexe en raison du volume croissant de données à gérer, ce qui rend difficile la mise en place de politiques de protection et de contrôle d'accès efficaces. Assurer une sensibilisation adéquate des employés à l'importance de la protection des données »*

La majorité des interviewés, dont I1, mettent en avant des défis tels que la gestion des accès et des autorisations, la protection contre les cybermenaces, ainsi que la sensibilisation et la formation continue du personnel. Cependant, une réponse plus technique est fournie par I2, qui renvoie à la sous-direction Informatique pour des détails supplémentaires. De même, I3 met en avant l'évolution des menaces de sécurité et la complexité des systèmes d'information comme des défis majeurs à relever. I4 souligne également la complexité croissante de la gestion des données électroniques, en raison du volume en constante augmentation, rendant ainsi difficile la mise en œuvre de politiques de protection et de contrôle d'accès efficaces. Il insiste sur l'importance d'assurer une sensibilisation adéquate des employés à la protection des données.

Figure 6: Nuage de mots correspondant à la confidentialité des Données (sensibilisation et défis)

Source : élaboré par nos soins

Selon le nuage de mots généré à partir l'analyse des entretiens, les termes les plus fréquemment évoqués par les participants incluent principalement la sécurité, données, accès, protection, sensible, autorisées, systèmes, contrôle, gestion, sensibles, protégé…etc.

III.2 Discussion des résultats

III.2.1 Compréhension de la Gouvernance Électronique

Selon les conclusions tirées des données recueillies et en référence à notre littérature, il est observé que la gouvernance électronique est largement conceptualisée comme une fusion de technologies visant à améliorer les prestations des services publics, en mettant en exergue des principes tels que l'efficience, la transparence, la responsabilité et l'inclusivité. Toutefois, bien que ces objectifs soient largement consensuels, des nuances apparaissent dans les définitions fournies par les participants, reflétant une diversité d'interprétations de la gouvernance électronique. Conformément à (Boudreau, 2011), la gouvernance électronique est définie

comme « L'exploitation des nouvelles technologies de l'information par les organisations publiques pour appuyer leurs fonctionnement internes et leurs interactions avec différentes parties prenantes et entités ». Cette citation met en lumière le rôle fondamental des technologies de l'information dans les opérations gouvernementales. Par ailleurs, Benyekhlef, dans son ouvrage sur l'administration publique en ligne au Canada (2004), souligne que « L'administration électronique, c'est-à-dire la prestation électronique de services, n'est qu'une des composantes nécessaires à la mise en place d'un gouvernement en ligne » (Benyekhlef, 2004) Cette remarque souligne la complexité de la transition vers un gouvernement en ligne, dépassant ainsi la simple prestation de services électroniques.

En outre, les participants reconnaissent généralement un niveau élevé d'adoption des politiques de gouvernance électronique au sein de la CNAS. Néanmoins, des défis persistants, tels que la résistance au changement et le besoin de maintenir les compétences des employés à jour face aux évolutions rapides des technologies, soulignent l'importance cruciale de la formation continue et de la communication efficace pour garantir le succès de la mise en œuvre de ces politiques. Ces résultats soulignent ainsi la nécessité de surmonter ces obstacles potentiels afin de maximiser les avantages de telles initiatives pour l'organisation.

III.2.2 Confidentialité des Données (sensibilisation et défis)

D'après les réponses, nous avons constaté que la CNAS considère la confidentialité des données comme très importante pour protéger les informations sensibles des assurés. Les différents responsables interrogés s'accordent à dire qu'il faut empêcher l'accès non autorisé, la divulgation, l'altération et la destruction des données. Pour cela, la CNAS a mis en place des politiques solides et utilise des technologies comme le chiffrement et les pares-feux pour protéger les données. Ils ont aussi un protocole strict en cas de problème, qui comprend la détection des incidents, l'isolation des systèmes affectés, l'évaluation des dommages, et la notification des autorités et des assurés.

Cependant, la CNAS doit relever des défis importants, notamment la gestion des systèmes d'information complexes et la protection contre les cyberattaques. La formation et la sensibilisation des employés sont essentielles pour créer une culture de sécurité. L'étude de Edward Snowden 2013 montre l'importance de contrôler strictement l'accès aux données et de

respecter les réglementations pour éviter les fuites de données. La CNAS doit rester vigilante et adapter ses stratégies de sécurité en permanence pour faire face aux nouvelles menaces, tout en s'assurant que les employés comprennent et suivent les politiques de confidentialité.

III.2.3 La confidentialité des données dans la gouvernance électronique dans la CNAS

Les services numériques proposés par la Caisse Nationale d'Assurance Sociale (CNAS) en Algérie dans le cadre de la gouvernance électronique incluent une variété d'initiatives visant à améliorer l'efficience et l'accessibilité des services publics. Parmi ces services, on trouve la dématérialisation des démarches administratives, la mise à disposition de portails en ligne pour les assurés, la gestion électronique des dossiers, ainsi que des plateformes de communication directe avec les assurés. Ces initiatives sont conçues pour simplifier les interactions entre les citoyens et l'administration, réduire les délais de traitement et accroître la transparence des services publics.

Pour assurer la confidentialité des données des assurés, la CNAS a mis en place plusieurs mesures techniques et organisationnelles. Les politiques de sécurité adoptées incluent l'utilisation de technologies de chiffrement pour protéger les informations sensibles en transit et au repos, ainsi que l'implémentation de pare-feu pour empêcher les accès non autorisés. En cas d'incident de sécurité, un protocole strict est suivi : détection rapide de l'incident, isolation des systèmes affectés, évaluation des dommages, et notification des autorités compétentes ainsi que des assurés potentiellement impactés.

Cependant, malgré ces précautions, la CNAS fait face à des défis significatifs. La gestion des systèmes d'information complexes et la protection contre les cyberattaques demeurent des préoccupations majeures. La résistance au changement parmi les employés et le besoin constant de mise à jour des compétences technologiques nécessitent une attention particulière. La formation continue et la sensibilisation des employés sont essentielles pour créer et maintenir une culture de sécurité robuste. Le cas d'Edward Snowden en 2013 a mis en évidence la nécessité de contrôles stricts sur l'accès aux données et le respect rigoureux des réglementations pour éviter les fuites de données.

En fin, les services numériques offerts par la CNAS dans le cadre de la gouvernance électronique sont conçus pour améliorer l'efficience et la transparence, tout en mettant en œuvre des mesures rigoureuses pour assurer la confidentialité des données des assurés. Toutefois, pour maximiser les avantages de ces initiatives, il est important de surmonter les obstacles liés à la gestion des systèmes d'information et à la protection contre les menaces de cybersécurité. L'adaptation continue des stratégies de sécurité et la formation des employés sont essentielles pour faire face aux nouvelles menaces et garantir que les politiques de confidentialité sont comprises et respectées. Ainsi, bien que la CNAS ait pris des mesures significatives pour protéger les données des assurés, une vigilance constante et des améliorations continues sont nécessaires pour assurer pleinement la confidentialité des données dans le cadre de la gouvernance électronique.

III.3 Les suggestions :

Sur la base des résultats obtenus et les défis identifiés, nous proposons quelques suggestions que la CNAS pourrait envisager pour renforcer la confidentialité des données des assurés dans le cadre de la gouvernance électronique :

- **Renforcer la sensibilisation et la formation :** Investir davantage dans des programmes de sensibilisation et de formation pour le personnel de la CNAS afin de garantir une compréhension approfondie des politiques de confidentialité des données et des procédures de sécurité. Cela pourrait aider à réduire les risques liés à la mauvaise manipulation des données et renforcer une culture de sécurité au sein de l'organisation

- **Mise à jour régulière des politiques de sécurité :** Réviser régulièrement les politiques de sécurité informatique pour s'adapter aux évolutions des menaces et des technologies, tout en s'assurant que ces politiques sont conformes aux normes et réglementations nationales et internationales en matière de protection des données.

- **Renforcement de la transparence et de la communication :** Communiquer de manière proactive avec les assurés sur les mesures prises pour protéger leurs données personnelles et sur les étapes à suivre en cas d'incident de sécurité.

III.4 Les limites de recherche :

1. Dépendance aux données disponibles ;
2. Evasion de répondre sur certaines questions ;
3. Le contexte socio-politique, notamment en ce qui concerne la confidentialité des données.

Ce chapitre a fourni une vue détaillée de la partie pratique de notre recherche. Nous avons commencé par la présentation des résultats qualitatifs obtenus grâce aux entretiens semi-directifs réalisés avec quatre participants. En utilisant la méthode d'analyse thématique et le logiciel Nvivo, nous avons pu analyser en profondeur ces données, révélant des tendances et des insights significatifs. Les résultats ont ensuite été examinés en détail, permettant de dégager des suggestions éclairées pour les futures recherches et les applications pratiques. Cette analyse approfondie renforce la validité et la pertinence de notre étude, offrant une base solide pour les conclusions et les recommandations ultérieures.

Conclusion générale

Conclusion

En somme, cette étude a mis en lumière les enjeux et défis liés à la confidentialité des données personnelles dans le cadre de la gouvernance électronique, en prenant comme étude de cas la Caisse Nationale des Assurances Sociales CNAS Tiaret. À travers une analyse approfondie, nous avons pu constater que la transformation numérique offre des opportunités significatives pour améliorer l'efficacité administrative et les services aux citoyens. Cependant, cette transition soulève également des questions cruciales concernant la protection des données personnelles.

Notre investigation a révélé que bien que la CNAS Tiaret ait fait des progrès notables dans la digitalisation de ses services, des lacunes subsistent en matière de protection des données. Les politiques actuelles, bien qu'alignées avec les régulations récentes, nécessitent des améliorations pour garantir une confidentialité optimale des informations des assurés. Le cadre juridique algérien, en évolution, apporte un soutien mais requiert une mise en œuvre rigoureuse pour instaurer une confiance durable entre les institutions et les citoyens.

La méthodologie qualitative adoptée, basée sur des entretiens directs, a permis de comprendre les perceptions et expériences des utilisateurs des services numériques de la CNAS. Les résultats indiquent une reconnaissance des bénéfices de la digitalisation, mais aussi des préoccupations persistantes sur la sécurité des données. Les recommandations formulées à l'issue de cette recherche visent à renforcer les politiques de confidentialité, améliorer la formation du personnel et sensibiliser les assurés sur le s enjeux de la protection des données.

On a constaté que la CNAS Tiaret puisse pleinement bénéficier des avantages de la gouvernance électronique tout en assurant la sécurité et la confidentialité des données, il est impératif de combiner une technologie avancée avec une réglementation rigoureuse et une gestion proactive des risques. Cette étude contribue ainsi à une meilleure compréhension des dynamiques entre digitalisation et protection des données dans le secteur public en Algérie, et propose des pistes concrètes pour une amélioration continue.

Bibliographie

Bibliographie

Alain, A. V. (2005). *Enjeux de mots : regards multiculturels sur les sociétés de l'information*. C & F Éditions.

BELLEIL. (2011). *E-privacy : le marché des données personnelles : protection de la vie privée à l'âge d'internet.* Paris: Dunod.

Brown, D. (2005). Le gouvernement électronique et l'administration publique. Revue internationale des sciences administratives (RISA). *251-266, 71(2).*

CASTETS-RENARD. (2015). *Quelle protection des données personnelles en Europe ?* Bruxelle. Récupéré sur Larcier.

FRAYSSINET, J. (2013). "La protection des données personnelles est-elle assurée sur l'Internet ?" . *G. CHATILLON, Le droit international de l'internet, Bruxellest*, 435.

Journal, W. S. (2019). *You Give Apps Sensitive Personal Information. Then They Tell Facebook* . Récupéré sur https ://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636

K, B. (2004). L'administration publique en ligne au Canada : précisions terminologiques et état de la réflexion' . *Revue Française d'administration publique*, 267.

LELEU, Y. (2018). *Droit des personnes et des familles, Bruxelles.* Larcier.

Misuraca, G. e. (2011). Measuring and Meta-Measuring, in Search of New Pathways for Modelling Impacts of ICT-enabled Services on the Information Society, Proceedings of the IFIP 8.5 eGOV2011. *Conference, Delft, Netherlands.*

Bibliographie

MUCCHIELLI, A. (1991). *Les méthodes qualitatives.* Paris: PUF.

Ossama, F. (2001). *Les nouvelles technologies de l'information : enjeux pour l'Afrique subsaharienne.* paris: Le Harmattan.

RAGOUCY, V. C. (2010). « Le panoptique et 1984 : confrontation de deux figures politiques d'asservissement ». *vol. 18*, 45-58.

Refafa.b. (2020). « La monétique en Algérie, développement et perspectives ». *Journal d'études en économie et Management, Volume 03 Numéro 06*.

Terranova. (2021). *Terranova Worldwide Corporation*. Récupéré sur TERRANOVASECURITY.COM,.

THIRION, N. (2011). *Théorie du droit : droit, pouvoir, savoir.* Bruxelles: Larcier.

Emad A. Abu-Shanab et Lana Q. Bataineh, « Challenges facing E-government project : How to avoid failure? », dans J. Emerg. Sci, Vol.4, N°4, 2014, Pages 207-217.

Samuel Warren et Louis Brandeis, L'article est publié en 1890 dans la Harvard Law Review. Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220.

F. RIGAUX, « La liberté de la vie privée », R.D.I.D.C., 1991, Vol. 43, pp. 539.

L'ICANN (« *Internet Corporation for Assigned Names and Numbers* ») se définit comme une organisation à but non lucratif et reconnue d'utilité publique rassemblant des participants du monde entier qui œuvrent à la préservation de la sécurité, la stabilité et l'interopérabilité de l'Internet : https ://www.icann.org/fr

Sunny, M., & James, D. M. (2003). E-Government and E-Governance: The future isn't what it used to be. Canadian Journal of Administrative Sciences, 20(01), p. 75

Bibliographie

Ossama, F. (2001). Les nouvelles technologies de l'information : enjeux pour l'Afrique subsaharienne, Paris, L'Harmattan.

https://publicadministration.un.org/egovkb/en-us/

J. FRAYSSINET, « La protection des données personnelles est-elle assurée sur l'Internet ? » in G. CHATILLON, Le droit international de l'internet, Bruxelles, Bruylant, 2013, p. 435.

Voy. C. RAGOUCY, « Le panoptique et 1984 : confrontation de deux figures politiques d'asservissement », Psychanalyse, vol. 18, 2010, pp. 45-58.

CASTETS-RENARD, Quelle protection des données personnelles en Europe ? Larcier, Bruxelles, 2015, p.30.

https://www.veritas.com/fr/ch/information-center/data-privacy, 2022

Annexes

Annexe A :

Guide d’entretien

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

Guide d'entretien

Bonjour monsieur, Je me nomme Mostefa DAHMANI, je suis étudiant en 2ème année master, spécialité : Management de l'e-gouvernement à l'Ecole Nationale Supérieure de Management (ENSM).

Je suis en phase finale de préparation de mon projet de fin d'étude sous le thème : Les défis liés à la confidentialité des données dans la gouvernance électronique : cas d'étude sur la CNAS. Pour cela, j'ai besoin de récolter des informations qui me permettent de traiter la problématique de recherche qui relie les deux concepts clés de mon étude « la gouvernance électronique » et « la confidentialité des données ».

Je tiens à vous assurer que toutes vos réponses seront anonymes et utilisées uniquement à des fins de recherche. Avec votre permission, puis-je enregistrer cet entretien pour faciliter la transcription ultérieure.

Partie 01 : Présentation de l'interviewé

- Pouvez-vous nous donner une brève présentation de la Caisse Nationale d'Assurance Sociale (CNAS) et de ses principales missions ?
- Quel est votre rôle au sein de la CNAS ?

Partie 02 : Les questions de l'entretien

Section 1 : Compréhension de la Gouvernance Électronique

1. Comment définiriez-vous la gouvernance électronique ?
2. Pour bien comprendre l'efficacité de la gouvernance électronique au sein de la CNAS, il est essentiel de savoir comment les politiques de gouvernance sont adoptées par la CNAS. Pourriez-vous nous parler du taux d'adoption des politiques de gouvernance au sein de la CNAS et quels sont les principaux défis que vous rencontrez à cet égard ?

3. Avez-vous des statistiques ou des indicateurs précis qui montrent le niveau d'adoption de ces politiques ?

4. Comment la formation continue des employés contribue-t-elle à l'adoption des politiques de gouvernance ?

5. Quel est le niveau de sensibilisation des employés de la CNAS à la gouvernance électronique ?

6. Quels sont les principaux défis que vous rencontrez pour sensibiliser les employés à la gouvernance électronique ?

Section 2 : Compréhension de la Gouvernance Électronique (sensibilisation et confidentialité)

1. Comment la CNAS définit-elle la confidentialité des données ?

2. Quelles politiques et procédures spécifiques avez-vous mises en place pour assurer la confidentialité des données ?

3. Quels types de technologies et d'outils utilisez-vous pour protéger la confidentialité des données ?

4. Quel est votre protocole en cas de violation de la confidentialité des données ?

5. Y a-t-il d'autres aspects de la confidentialité des données que vous aimeriez aborder?

6. Quels sont les principaux défis rencontrés par la CNAS en matière de protection de la confidentialité des données dans le cadre de la gouvernance électronique

Clôture

Remerciements

Remerciez l'interviewer pour son temps et ses contributions.

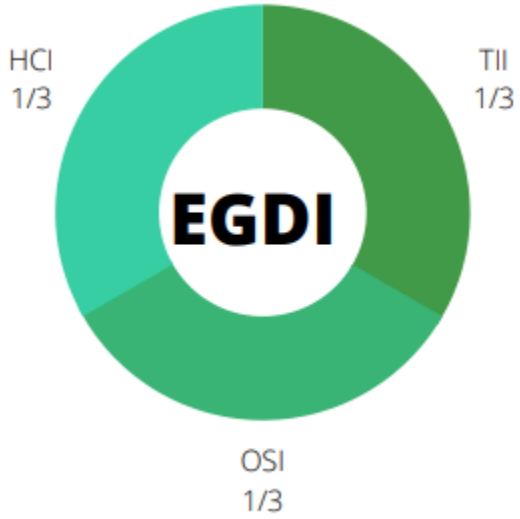
Annexe B :

L'EGDI

L’index de développement du e-gouvernement (EGDI) a été créé par l'United Nations Department of Economic and Social Affairs (UN DESA), il permet aux 193 membres des Nations Unies de comparer leur performance en matière de egouvernement et d'identifier les domaines où des progrès supplémentaires sont nécessaires. Il est basé sur 32 indicateurs répartis sur trois dimensions :

1. La portée et la qualité des services en ligne (Online Service Index, OSI).
2. L’état de développement de l'infrastructure de télécommunication (Indice de l'infrastructure des télécommunications, TII).
3. Le capital humain (Indice du capital humain, HCI).

L'EGDI ne représente pas une mesure absolue du développement de l'e-gouvernement



dans un pays mais il vise plutôt à comparer les performances des gouvernements les uns par rapport aux autres.

Mathématiquement, l'EGDI est une moyenne pondérée de trois scores normalisés sur les trois dimensions :

EGDI =1/3 (OSI + TII + HCI)

La valeur est comprise entre 0 et 1

Annexe C :

RANSOMWARE (RANÇONGICIEL)

Des logiciels malveillants qui peuvent s'infiltrer dans vos ordinateurs Qu'est-ce qu'un rançongiciel ou ransomware ? Précision sur le mode opératoire Un ransomware, ou rançongiciel, est un logiciel malveillant, prenant en otage les données. Il infecte les ordinateurs, chiffre les fichiers contenus dans le système infecté et demande une rançon (en cryptomonnaie) en échange d'une clé ou d'un mot de passe permettant de les déchiffrer.

PRÉVENTION

1. Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine.
2. Tenez à jour l'antivirus et configurez votre pare-feu. Vérifiez qu'il ne laisse passer que des applications, services et machines légitimes.
3. N'ouvrez pas les courriels, leurs pièces jointes et ne cliquez par sur les liens provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu, mais dont la structure du message est inhabituelle ou vide.
4. N'installez pas d'application ou de programme « piratés » ou dont l'origine ou la réputation sont douteuses.
5. Évitez les sites non sûrs ou illicites tels ceux hébergeant des contrefaçons (musique, films, logiciels…) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.
6. Faites des sauvegardes régulières de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine au besoin.
7. N'utilisez pas un compte avec des droits « administrateur » pour consulter vos messages ou naviguer sur Internet.
8. Utilisez des mots de passe suffisamment complexes et changez-les régulièrement, mais vérifiez également que ceux créés par défaut soient effacés s'ils ne sont pas tout de suite changés.
9. Éteignez votre machine lorsque vous ne vous en servez pas.

Source : plateforme Cybermalveillance.gouv.fr

Je suis victime de rançongiciels (ransomwares), que faire ?

- ✓ Débranchez la machine d'internet ou du réseau Informatique.
- ✓ Isolez les supports touchés par le Ransomware.
- ✓ En entreprise, alertez immédiatement votre service informatique.
- ✓ Ne payez pas la rançon, vous alimenteriez le système mafieux, sans certitude de récupérer les données.
- ✓ Déposez plainte auprès de la police ou de la gendarmerie ou en écrivant au procureur de la République dont vous dépendez.