UNIVERSITE CADI AYYAD
MARRAKECH

جامعة القاضي عياض
مراكش

Faculté des Sciences et Techniques Guéliz – Marrakech

Module : Fondamentaux de la sécurité informatique et cyber droit

Cadre réglementaire en France de la sécurité des Systèmes d'information et de la confiance numérique

Élèves ingénieur

El Mahdaoui Mohamed

Enseignant

SADQI Yassine

Table de contenue

Introduction

Dans une société à la fois globalement interconnectée et pleinement en situation de dépendance numérique manifeste, la sécurité, non seulement des systèmes d'information, mais aussi de la confiance numérique s'est, au fil des ans, imposée comme un enjeu central, voire déterminant pour les États, pour les entreprises, ainsi que pour les citoyens eux-mêmes. Consciente de ces enjeux, la France a conçu, pour faire face, un cadre réglementaire ambitieux structurellement fondée sur un environnement numérique « sécurisé », « fiable » et « propice au développement économique et social », établi autour des principaux piliers de la sécurité des systèmes d'information et de la confiance numérique.

C'est à la faveur du recours exponentiel aux technologies numériques dans tous les secteurs de l'activité, étayé par la sophistication croissante des cybermenaces, que l'État français doit faire le pari d'une intervention proactive, qui se traduira par la définition d'exigences minimales d'ordre organisationnel, technique et contractuels applicables aux systèmes d'information, en tenant compte des particularités et enjeux de sécurité de chaque domaine. Ce premier choix conduit d'une part à assurer la protection des informations les plus sensibles, d'autre part, à garantir la continuité des services dits « essentiels » au bon fonctionnement de la Nation.

Au-delà des obligations des différents acteurs publics et privés, le cadre réglementaire français consacrera en outre le rôle pivot de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), autorité nationale de la sécurité et de la défense des systèmes d'information, participant à la détection, à la prévention et à la réponse aux incidents de sécurité et à l'accompagnement des acteurs à une meilleure posture de cybersécurité.

Ce rapport vise à fournir une analyse approfondie du cadre réglementaire français en matière de sécurité des systèmes d'information et de confiance numérique, selon les deux grands champs d'application identifiés, en décrivant les principales réglementations, leurs objectifs, leur portée et leurs conséquences pour les acteurs concernés : les textes législatifs et réglementaires, les directives européennes transposées, les référentiels normatifs constituant cet écosystème complexe et mouvant.

partie 1 : Le Cadre Réglementaire de la Sécurité des Systèmes d'Information

1.1. Introduction au Cadre Réglementaire SSI

Le cadre réglementaire français de la sécurité des systèmes d'information (SSI) se façonne progressivement, en réponse à des évolutions technologiques et de menaces qui se sont révélées fulgurantes. Comme indiqué dans l'introduction, la croissance exponentielle de l'usage des systèmes d'informations conjuguée à l'accroissement des menaces qui les visent a conduit l'État à investir activement le champ du numérique. À travers cette montée en puissance, l'objectif recherché est de construire un ensemble de règles et de normes minimales permettant de sécuriser les systèmes concernés tout en tenant compte des enjeux sectoriels et des niveaux de sensibilité d'information traitée spécifiques à chacun.

La façon d'aborder la SSI en France se veut globale en incluant tant la protection de données particulièrement sensibles, tels les secrets de la défense nationale, que les conditions de continuité des services jugés indispensables à la nation. Cette double préoccupation se reflète d'ailleurs dans la diversité des réglementations mises en œuvre, ciblant un panel d'acteurs et de systèmes d'information variés.

Un élément essentiel de ce cadre réglementaire SSI est la définition du rôle même de l'ANSSI. En plus des missions de détection et de réponse aux incidents, elle est aussi animée par la définition et la diffusion de bonnes pratiques ou référentiels de sécurité, et par l'accompagnement des acteurs dans la mise en œuvre des mesures de sécurité nécessaires, tandis que la réglementation restreint le champ des capacités de l'ANSSI à détecter tel ou tel événement pouvant affecter la sécurité des systèmes d'information des différentes entités. Cela met en évidence son rôle prépondérant dans le contrôle et la protection du cyberespace national.

Le cadre réglementaire relatif à la sécurité des systèmes d'information peut être structuré en cinq grandes catégories, permettant une approche méthodique et sectorielle de la cybersécurité :

1. **La protection du secret** : Concerne la protection des informations classifiées et relevant du secret de la défense nationale, un pilier fondamental de la sécurité de l'État.

2. **La protection des informations sensibles et à diffusion restreinte** : Vise à protéger les informations qui, sans être classifiées secret défense, nécessitent néanmoins un niveau de protection élevé en raison de leur sensibilité pour les intérêts nationaux ou économiques.

3. **La protection des systèmes d'information des Opérateurs d'Importance Vitale (OIV), des Opérateurs de Services Essentiels (OSE), des Fournisseurs de Services Numériques (FSN), des Entités Importantes (EI) et des Entités Essentielles (EE)** : Cible

les acteurs critiques dont l'activité est essentielle au fonctionnement de la société et de l'économie, et qui sont donc particulièrement exposés aux cybermenaces.

4. **La protection des systèmes d'information de l'État** : Porte spécifiquement sur la sécurisation des systèmes d'information des administrations et établissements publics de l'État, garantissant ainsi la continuité des services publics et la protection des données gouvernementales.

5. **La détection** : Englobe les dispositifs et les mécanismes mis en place pour détecter les incidents de sécurité, un aspect crucial pour une réponse rapide et efficace aux cyberattaques.

1.2. La protection du secret

La protection du secret constitue un pilier fondamental de la sécurité des systèmes d'information en France, en particulier lorsqu'il s'agit de la défense nationale et des intérêts stratégiques de l'État. Ce domaine est encadré par un ensemble d'instructions interministérielles qui définissent les exigences applicables aux informations et supports classifiés, ainsi qu'aux moyens et mesures de protection associés. Ces instructions visent à garantir la confidentialité, l'intégrité et la disponibilité des informations sensibles, en prévenant leur divulgation, leur altération ou leur perte.

1.2.1. L'Instruction Générale Interministérielle 1300 (IGI 1300) :

Cette instruction est la pierre angulaire du dispositif de protection du secret de la défense nationale en France. Elle définit de manière exhaustive les exigences applicables aux **informations et supports soumis au secret de la défense nationale (classifiés)**. L'IGI 1300 couvre l'ensemble du cycle de vie des informations classifiées, depuis leur création ou réception jusqu'à leur destruction, en passant par leur stockage, leur transmission et leur consultation.

- **Objectifs et portée :** L'objectif principal de l'IGI 1300 est de protéger les informations classifiées, dont la divulgation pourrait nuire à la défense nationale ou aux intérêts fondamentaux de la nation. Elle s'applique à toutes les administrations publiques, les organismes privés et les personnes physiques ou morales qui sont amenés à manipuler des informations classifiées dans le cadre de leurs activités. Elle couvre un large éventail de supports, allant des documents papier aux données numériques, en passant par les matériels et les logiciels.

- **Principales exigences :** L'IGI 1300 établit un cadre de classification des informations en différents niveaux de secret (Très Secret Défense, Secret Défense, Confidentiel Défense, Diffusion Restreinte - bien que "Diffusion Restreinte" soit plus souvent associée à la protection des informations sensibles non classifiées secret défense). Elle précise les règles d'habilitation des personnes autorisées à accéder aux informations classifiées, les procédures de manipulation et de protection des supports, les mesures de sécurité physique et logique à mettre en œuvre, ainsi que les modalités de contrôle et de sanction

en cas de manquement. L'IGI 1300 impose également des exigences en matière de système d'information, notamment en termes de sécurité des réseaux, de contrôle d'accès, de journalisation et de gestion des incidents de sécurité. Elle détaille les responsabilités des différents acteurs, depuis le chef d'organisme jusqu'aux agents manipulant des informations classifiées.

1.2.2. L'Instruction Interministérielle 910 (IMI 910) :

L'IMI 910 se concentre sur la **mise en œuvre et la gestion des articles contrôlés de la sécurité des systèmes d'information**. Les "articles contrôlés" font référence aux produits et technologies de sécurité (matériels, logiciels, services) qui sont considérés comme sensibles ou stratégiques et dont l'utilisation est soumise à un contrôle réglementaire. Ces contrôles visent à garantir que ces produits sont utilisés de manière appropriée et ne sont pas détournés à des fins malveillantes ou contraires aux intérêts nationaux.

- **Objectifs et portée :** L'IMI 910 vise à encadrer l'utilisation des articles contrôlés de sécurité des systèmes d'information. Elle s'applique aux organismes publics et privés qui déploient ou utilisent ces produits dans le cadre de la protection de leurs systèmes d'information, notamment ceux traitant des informations classifiées ou sensibles. Elle couvre un large éventail de produits, tels que les dispositifs de chiffrement, les systèmes de détection d'intrusion, les pares-feux, les solutions d'authentification forte, etc.
- **Principales exigences :** L'IMI 910 définit les procédures d'acquisition, de déploiement, de configuration, d'exploitation et de maintenance des articles contrôlés. Elle impose des exigences en matière de qualification et d'habilitation du personnel chargé de la gestion de ces produits, ainsi que des règles de sécurité physique et logique pour leur protection. Elle précise également les modalités de contrôle et d'audit de l'utilisation des articles contrôlés, ainsi que les responsabilités des différents acteurs impliqués. L'IMI 910 est souvent appliquée en complément de l'IGI 1300 pour la sécurisation des systèmes d'information traitant des informations classifiées.

1.2.3. L'Instruction Interministérielle 300 (IMI 300) :

L'IMI 300 est dédiée à la **protection contre les signaux compromettants**. Les signaux compromettants (également appelés émanations électromagnétiques) sont des émissions involontaires d'énergie électromagnétique provenant des équipements électroniques qui peuvent potentiellement être captées et exploitées pour reconstituer les informations traitées. L'IMI 300 vise à prévenir ce type de compromission, en particulier pour les informations classifiées ou sensibles.

- **Objectifs et portée :** L'objectif de l'IMI 300 est de protéger les informations sensibles contre la compromission par le biais des signaux compromettants. Elle s'applique aux organismes publics et privés qui traitent des informations classifiées ou sensibles dans des zones considérées comme sensibles ou à risque. Elle concerne tous les types d'équipements électroniques susceptibles d'émettre des signaux compromettants, tels que les ordinateurs, les serveurs, les téléphones, les périphériques, etc.

- **Principales exigences :** L'IMI 300 définit les mesures de protection à mettre en œuvre pour atténuer ou masquer les signaux compromettants. Ces mesures peuvent être de nature technique (blindage, filtrage, mise à la terre, etc.), organisationnelle (contrôle d'accès, zones protégées, etc.) ou procédurale (gestion des équipements, sensibilisation du personnel, etc.). L'IMI 300 impose également des exigences en matière de tests et d'évaluation des mesures de protection, ainsi que de surveillance et de maintenance des équipements et des installations. Elle peut impliquer la mise en place de zones TEMPEST (Telecomunications Electronics Material Protected from Emanating Spurious Transmissions) pour les environnements les plus sensibles.

1.2.4. L'Instruction Interministérielle 2100 (IMI 2100) :

L'IMI 2100 précise les particularités liées aux rôles et responsabilités associées ainsi qu'aux exigences applicables à la protection en France des informations ou supports classifiés émis dans le cadre de l'OTAN. Elle vient compléter l'IGI 1300 en adaptant ses dispositions au contexte spécifique des informations classifiées OTAN.

- **Objectifs et portée :** L'objectif de l'IMI 2100 est d'assurer la protection des informations classifiées OTAN en France, conformément aux accords et aux normes de l'OTAN. Elle s'applique aux organismes publics et privés français qui sont amenés à manipuler des informations classifiées OTAN dans le cadre de leur coopération avec l'OTAN ou avec les États membres de l'OTAN. Elle couvre tous les types d'informations classifiées OTAN, quel que soit leur niveau de classification (COSMIC TOP SECRET, NATO SECRET, NATO CONFIDENTIAL, NATO RESTRICTED).
- **Principales exigences :** L'IMI 2100 reprend les principes généraux de l'IGI 1300 mais les adapte aux spécificités du contexte OTAN. Elle précise les rôles et responsabilités des différents acteurs français dans la gestion des informations classifiées OTAN, notamment en matière d'habilitation, de contrôle d'accès, de transmission et de destruction. Elle impose également des exigences spécifiques en matière de systèmes d'information, de sécurité physique et de protection contre les signaux compromettants, conformes aux normes de l'OTAN. L'IMI 2100 assure la cohérence du dispositif français de protection du secret avec les exigences de l'OTAN.

1.2.5. L'Instruction Générale Interministérielle 2102 (IGI 2102) :

De manière similaire à l'IMI 2100 pour l'OTAN, l'IGI 2102 précise les particularités liées aux rôles et responsabilités associées ainsi qu'aux exigences applicables à la protection en France des informations ou supports classifiés de l'Union européenne. Elle adapte également l'IGI 1300 au contexte spécifique des informations classifiées de l'Union Européenne.

- **Objectifs et portée :** L'objectif de l'IGI 2102 est d'assurer la protection des informations classifiées de l'Union européenne en France, conformément aux règles et aux normes de l'UE. Elle s'applique aux organismes publics et privés français qui sont amenés à manipuler des informations classifiées de l'UE dans le cadre de leur participation aux activités de l'UE ou de leur coopération avec les institutions et les États membres de l'UE. Elle couvre tous

les types d'informations classifiées de l'UE, quel que soit leur niveau de classification (EU TOP SECRET, EU SECRET, EU CONFIDENTIAL, EU RESTRICTED).

- **Principales exigences :** L'IGI 2102 reprend les principes généraux de l'IGI 1300 en les adaptant au contexte de l'UE. Elle précise les rôles et responsabilités des acteurs français dans la gestion des informations classifiées de l'UE, notamment en matière d'habilitation, de contrôle d'accès, de transmission et de destruction. Elle impose également des exigences spécifiques en matière de systèmes d'information, de sécurité physique et de protection contre les signaux compromettants, conformes aux normes de l'UE. L'IGI 2102 assure la cohérence du dispositif français de protection du secret avec les exigences de l'Union européenne.

1.2.6. En résumé

La protection du secret en France repose sur un cadre réglementaire robuste et détaillé, centré autour de l'IGI 1300 et complété par des instructions spécifiques pour les articles contrôlés, les signaux compromettants, les informations classifiées OTAN et les informations classifiées de l'Union européenne. Ces instructions définissent un ensemble d'exigences techniques, organisationnelles et procédurales visant à garantir la confidentialité des informations les plus sensibles pour la sécurité nationale et les intérêts stratégiques de la France.

1.3. La protection des informations sensibles et à diffusion restreinte

Au-delà de la protection du secret de la défense nationale, le cadre réglementaire français de la SSI prend également en compte la nécessité de protéger les **informations sensibles et à diffusion restreinte**. Ces informations, bien que ne relevant pas du niveau de classification "secret défense", n'en demeurent pas moins critiques pour les intérêts de l'État, des entreprises ou des citoyens. Leur divulgation, leur altération ou leur perte pourraient avoir des conséquences préjudiciables, justifiant ainsi la mise en place de mesures de protection spécifiques.

Cette catégorie de protection s'articule principalement autour de deux dispositifs réglementaires majeurs :

1.3.1. Le Dispositif de Protection du Patrimoine Scientifique et Technique (PPST) instauré par le décret n° 2011-245 :

Le PPST est un dispositif spécifique visant à protéger le patrimoine scientifique et technique **(PST)** de la nation, qui représente un enjeu stratégique majeur pour la compétitivité, l'innovation et la souveraineté de la France. Le décret n° 2011-245 du 3 mars 2011, relatif à la protection du potentiel scientifique et technique de la nation, met en place ce dispositif et définit notamment le cadre des zones à régime restrictif **(ZRR)**.

- **Objectifs et portée :** L'objectif principal du PPST est de prévenir les atteintes au patrimoine scientifique et technique national, notamment les risques d'espionnage économique, de captation de technologies sensibles ou de pillage de savoir-faire stratégiques. Il s'applique aux établissements intervenant dans des secteurs scientifiques et techniques protégés, tels que la défense, l'énergie nucléaire, l'aérospatiale, les biotechnologies, etc. Le champ d'application du PPST est défini par arrêté interministériel, qui précise les secteurs d'activité concernés et les types de PST à protéger.
- **Principales exigences :** Le décret n° 2011-245 instaure le concept de zones à régime restrictif (ZRR) au sein des établissements concernés. Les ZRR sont des zones géographiques ou fonctionnelles dans lesquelles l'accès, la circulation, l'activité et la détention d'objets ou d'informations sont soumis à des règles spécifiques de sécurité. Le décret définit les modalités de création, de délimitation et de gestion des ZRR, ainsi que les obligations des établissements en matière de sécurité physique, de contrôle d'accès, de protection des informations et de sensibilisation du personnel. Il prévoit également des procédures d'autorisation et de contrôle des activités menées dans les ZRR. Le PPST est un dispositif essentiel pour la protection de la recherche et de l'innovation françaises face aux menaces extérieures.

1.3.2. L'Instruction Interministérielle 901 (IMI 901) :

L'IMI 901 définit les exigences organisationnelles et techniques applicables aux systèmes d'information sensibles ou « Diffusion Restreinte ». Elle s'adresse aux systèmes d'information qui traitent des informations sensibles, mais non classifiées secret défense, et qui nécessitent un niveau de protection adapté à leur sensibilité. La mention "Diffusion Restreinte" est souvent utilisée pour qualifier ce type d'informations, qui ne sont pas destinées à être diffusées largement et dont l'accès doit être contrôlé.

- **Objectifs et portée :** L'objectif de l'IMI 901 est de garantir la sécurité des systèmes d'information traitant des informations sensibles ou "Diffusion Restreinte", en définissant un cadre de référence pour la mise en œuvre de mesures de sécurité proportionnées aux risques. Elle s'applique aux administrations publiques, aux organismes privés et aux opérateurs d'importance vitale (OIV) qui traitent ce type d'informations. Le périmètre exact des informations "Diffusion Restreinte" peut varier en fonction des contextes et des secteurs d'activité, mais il s'agit généralement d'informations dont la divulgation pourrait porter atteinte aux intérêts économiques, financiers, commerciaux, industriels, scientifiques, sociaux, environnementaux ou à la vie privée des personnes.
- **Principales exigences :** L'IMI 901 établit un ensemble d'exigences organisationnelles et techniques pour la sécurité des systèmes d'information sensibles. Parmi les exigences organisationnelles, on retrouve la désignation d'un responsable de la sécurité des systèmes d'information (RSSI), la mise en place d'une politique de sécurité, la gestion des risques, la sensibilisation et la formation du personnel, la gestion des habilitations d'accès, la gestion des incidents de sécurité et la mise en place de plans de continuité d'activité (PCA). Parmi les exigences techniques, l'IMI 901 couvre un large spectre de domaines, tels

que la sécurité physique des locaux, la sécurité des réseaux, la sécurité des systèmes et des applications, la protection des données, la gestion des identités et des accès, la journalisation et l'audit de sécurité, la gestion de la configuration et des changements, et la sécurité des échanges avec les tiers. L'IMI 901 s'appuie sur des référentiels de bonnes pratiques et des normes de sécurité reconnues, tels que les normes ISO 27001 et ISO 27002. Elle permet aux organismes de définir et de mettre en œuvre un système de management de la sécurité de l'information (SMSI) adapté à leurs besoins et à leurs risques.

1.3.3. En résumé

la protection des informations sensibles et à diffusion restreinte en France s'appuie sur deux piliers principaux : le PPST, qui vise à protéger le patrimoine scientifique et technique national au travers des ZRR, et l'IMI 901, qui définit les exigences de sécurité pour les systèmes d'information traitant des informations sensibles ou "Diffusion Restreinte". Ces dispositifs permettent de garantir un niveau de protection adapté aux informations qui, sans être classifiées secret défense, n'en demeurent pas moins importantes pour les intérêts de la nation et des acteurs économiques.

1.4. La protection des systèmes d'information des OIV, des OSE et FSN et des EI et EE

La protection des systèmes d'information des Opérateurs d'Importance Vitale (OIV), des Opérateurs de Services Essentiels (OSE), des Fournisseurs de Services Numériques (FSN), des Entités Importantes (EI) et des Entités Essentielles (EE) représente un enjeu majeur du cadre réglementaire français de la SSI. Ces acteurs, par la nature de leurs activités, sont essentiels au fonctionnement de la nation, de son économie et de la vie quotidienne des citoyens. Les cyberattaques les visant peuvent avoir des conséquences graves et systémiques, justifiant une attention particulière et des obligations réglementaires renforcées en matière de cybersécurité.

Ce cadre réglementaire s'est construit progressivement, en réponse à l'évolution des menaces et à la reconnaissance de la criticité croissante de certains secteurs d'activité. Il s'articule autour de plusieurs textes législatifs et réglementaires, dont les principaux sont :

1.4.1. La Loi de Programmation Militaire 2014-2019 (LPM 2014-2019) et le code de la défense :

La LPM 2014-2019 a introduit dans le code de la défense un dispositif spécifique pour renforcer la sécurité des systèmes d'information d'importance vitale (SIIV) mis en œuvre par les **Opérateurs d'Importance Vitale (OIV)**. Ce fut la première étape majeure de la réglementation française ciblant spécifiquement les infrastructures critiques.

- **Objectifs et portée :** L'objectif de la LPM 2014-2019 et du dispositif OIV est de garantir la continuité des activités vitales de la nation en renforçant la cybersécurité des systèmes d'information des opérateurs qui les mettent en œuvre. Les OIV sont des organismes publics ou privés exerçant des activités critiques dans des secteurs vitaux tels que l'énergie, les transports, la santé, les finances, l'eau, l'alimentation, les télécommunications, l'industrie de défense, l'administration de l'État, etc. La liste des secteurs d'activité vitaux et la désignation des OIV sont définies par décret.
- **Principales exigences :** Le code de la défense, suite à la LPM 2014-2019, impose aux OIV un ensemble d'obligations en matière de sécurité de leurs SIIV. Ces obligations comprennent :
    - **La désignation d'un responsable de la sécurité des systèmes d'information (RSSI) OIV** : chargé de piloter la politique de sécurité et de veiller à sa mise en œuvre.
    - **La réalisation d'audits de sécurité périodiques de leurs SIIV** : pour évaluer le niveau de sécurité et identifier les vulnérabilités.
    - **La mise en œuvre de règles de sécurité définies par l'ANSSI** : des règles techniques et organisationnelles minimales à respecter pour protéger les SIIV. Ces règles sont précisées dans des arrêtés ministériels et des guides de l'ANSSI.
    - **La notification des incidents de sécurité significatifs à l'ANSSI** : pour permettre à l'ANSSI de coordonner la réponse aux incidents et de disposer d'une vision globale de la menace.
    - **La mise en place de mesures de sécurité physique et logique** : pour protéger les SIIV contre les accès non autorisés, les intrusions, les pertes de données, les interruptions de service, etc.
    - **La réalisation d'exercices de crise et de tests d'intrusion** : pour évaluer la capacité de l'OIV à faire face à des cyberattaques.

Le dispositif OIV a constitué une avancée majeure dans la prise en compte de la cybersécurité des infrastructures critiques en France, en imposant des obligations concrètes et contrôlables aux opérateurs concernés.

1.4.2. La Directive NIS (Network and Information Security Directive) et sa transposition en droit français :

La directive (UE) 2016/1148, dite directive NIS, est la première directive européenne visant à renforcer la cybersécurité au niveau de l'Union européenne. Elle a été transposée en droit français par l'ordonnance n° 2018-314 du 25 avril 2018 et le décret n° 2018-351 du 14 mai 2018. La directive NIS a introduit les concepts d'**Opérateurs de Services Essentiels (OSE)** et de **Fournisseurs de Services Numériques (FSN)**, élargissant le champ de la réglementation au-delà des seuls OIV.

- **Objectifs et portée :** La directive NIS vise à améliorer le niveau global de cybersécurité dans l'UE en établissant des exigences minimales pour les OSE et les FSN. Les OSE sont des entités publiques ou privées fournissant des services essentiels pour la société et l'économie, dans des secteurs tels que l'énergie, les transports, la banque, les infrastructures numériques, la santé, l'eau potable et les infrastructures numériques. La directive NIS a défini une liste de secteurs et de sous-secteurs pour les OSE. Les FSN sont des entités fournissant des services numériques tels que les places de marché en ligne, les moteurs de recherche en ligne et les services d'informatique en nuage.
- **Principales exigences :** La directive NIS impose aux États membres de désigner les OSE et les FSN relevant de leur juridiction, et de leur imposer un ensemble d'obligations en matière de cybersécurité. Ces obligations comprennent :
    - **La prise de mesures de sécurité appropriées et proportionnées aux risques** : pour assurer la sécurité des réseaux et des systèmes d'information qu'ils utilisent pour fournir leurs services essentiels ou numériques. Ces mesures doivent être basées sur une approche par les risques et prendre en compte l'état de l'art en matière de cybersécurité.
    - **La notification des incidents de sécurité ayant un impact significatif sur la continuité des services essentiels ou numériques** : aux autorités compétentes désignées par les États membres (en France, l'ANSSI). La directive NIS précise les critères permettant de déterminer si un incident est significatif et doit être notifié.
    - **La coopération avec les autorités compétentes et les autres États membres** : pour échanger des informations sur les menaces et les incidents de sécurité, et pour coordonner les actions de réponse.

La transposition de la directive NIS en France a permis d'élargir le champ de la réglementation cybersécurité aux OSE et aux FSN, et d'harmoniser les exigences au niveau européen. Elle a renforcé le rôle de l'ANSSI en tant qu'autorité compétente pour la mise en œuvre de la directive et la supervision des OSE et des FSN.

1.4.3. En résume

La protection des systèmes d'information des OIV, des OSE, des FSN, des EI et des EE est un domaine central du cadre réglementaire français de la SSI. Il a évolué progressivement, en commençant par le dispositif OIV introduit par la LPM 2014-2019, puis en s'élargissant avec la transposition de la directive NIS. Ce cadre réglementaire vise à garantir un niveau élevé de cybersécurité pour les acteurs critiques de la société et de l'économie, en imposant des obligations concrètes en matière de sécurité, de notification d'incidents, de supervision et de sanctions.

1.5. La protection des systèmes d'information de l'État

La protection des systèmes d'information de l'État (SIE) constitue un volet essentiel du cadre réglementaire français de la SSI. L'État, en tant que premier détenteur et utilisateur de données sensibles et opérateur de services publics numériques, est une cible privilégiée pour les cyberattaques. Garantir la sécurité de ses systèmes d'information est donc une priorité absolue pour assurer la continuité des services publics, la protection des données des citoyens et la souveraineté numérique de la France.

Le cadre réglementaire spécifique aux SIE est principalement défini par deux textes majeurs mention :

1.5.1. Le Décret n° 2022-513 du 8 avril 2022 :

Ce décret, relatif à la gouvernance de la sécurité numérique de l'État, constitue un texte fondateur pour l'organisation et le pilotage de la cybersécurité au sein de l'administration publique française. Il définit le cadre de **gouvernance de la sécurité numérique des administrations et établissements publics d'État**.

- **Objectifs et portée :** L'objectif principal du décret n° 2022-513 est d'établir une gouvernance claire, structurée et efficace de la sécurité numérique au sein de l'État. Il vise à renforcer la coordination, la mutualisation et la professionnalisation de la cybersécurité dans l'ensemble de l'administration publique. Le décret s'applique à toutes les administrations centrales et déconcentrées de l'État, ainsi qu'aux établissements publics d'État, à l'exception de certaines catégories spécifiques (telles que les établissements de santé et les établissements d'enseignement supérieur et de recherche, qui peuvent être soumis à des régimes spécifiques).
- **Principales dispositions :** Le décret n° 2022-513 met en place plusieurs mécanismes clés pour la gouvernance de la sécurité numérique de l'État :
    - **La création d'un Comité Ministériel de la Sécurité Numérique (CMSN)** : présidé par le Premier ministre et composé des ministres concernés par la sécurité numérique. Le CMSN définit les orientations stratégiques de la politique de sécurité numérique de l'État, valide les documents de référence et assure le pilotage interministériel de la cybersécurité.
    - **La désignation d'un Haut Fonctionnaire de Défense et de Sécurité (HFDS) au sein de chaque ministère** : le HFDS est responsable de la mise en œuvre de la politique de sécurité numérique au sein de son ministère, et assure la coordination avec les autres ministères et les services compétents (notamment l'ANSSI).
    - **La désignation d'un Responsable Ministériel de la Sécurité des Systèmes d'Information (RMSSI) au sein de chaque ministère** : le RMSSI est l'expert en cybersécurité du ministère, chargé de piloter la politique de sécurité des systèmes d'information ministériels, de coordonner les actions de sécurité et de rendre compte au HFDS et au CMSN.

- **La création d'un réseau des RMSSI** : animé par l'ANSSI, ce réseau permet l'échange d'informations, le partage de bonnes pratiques et la mutualisation des moyens entre les RMSSI des différents ministères.
- **La définition d'un cadre commun de référence pour la sécurité numérique de l'État** : ce cadre est précisé dans la Politique de Sécurité des Systèmes d'Information de l'État (PSSIE) (voir point suivant).
- **La mise en place de mécanismes de pilotage, de suivi et d'évaluation de la sécurité numérique de l'État** : l'ANSSI assure un rôle central dans ce pilotage, en réalisant des audits, des contrôles, des analyses de risques et en produisant des rapports réguliers sur l'état de la sécurité numérique de l'État.

Le décret n° 2022-513 vise à instaurer une culture de la cybersécurité au sein de l'administration publique, à renforcer les compétences et les moyens dédiés à la sécurité numérique, et à améliorer la capacité de l'État à prévenir, détecter et répondre aux cyberattaques.

1.5.2. La Politique de Sécurité des Systèmes d'Information de l'État (PSSIE) :

La PSSIE est le document de référence qui précise le cadre commun de référence pour la sécurité numérique de l'État mentionné dans le décret n° 2022-513. Elle définit les principes, les objectifs, les règles et les mesures de sécurité applicables à l'ensemble des systèmes d'information des administrations et établissements publics d'État. La PSSIE est élaborée par l'ANSSI, en concertation avec les ministères, et validée par le CMSN.

- **Objectifs et portée :** L'objectif de la PSSIE est de fournir un cadre normatif et méthodologique unique pour la sécurité des SIE, permettant d'assurer un niveau de sécurité homogène et cohérent dans l'ensemble de l'administration publique. Elle s'adresse à tous les acteurs de la sécurité numérique de l'État, des décideurs politiques aux agents opérationnels, et couvre tous les aspects de la sécurité des systèmes d'information, qu'ils soient organisationnels, techniques ou humains.
- **Principaux axes et exigences :** La PSSIE s'articule autour de plusieurs axes majeurs et définit un ensemble d'exigences détaillées, couvrant notamment :
  - **La gouvernance de la sécurité des systèmes d'information** : précisant les rôles et responsabilités des différents acteurs, les instances de pilotage et de décision, les processus de gestion des risques, de gestion des incidents, de gestion de crise, etc.
  - **La sécurité physique et environnementale** : définissant les mesures de protection des locaux, des infrastructures et des équipements hébergeant les SIE.
  - **La sécurité logique** : couvrant la gestion des identités et des accès, l'authentification, l'autorisation, la journalisation et l'audit de sécurité, la sécurité des réseaux, des systèmes et des applications, la protection des données, la cryptographie, etc.

- **La sécurité humaine** : portant sur la sensibilisation et la formation du personnel, la gestion des habilitations, la sécurité des prestataires externes, la lutte contre la malveillance interne, etc.
- **La gestion des crises de cybersécurité et la continuité d'activité** : définissant les plans de gestion de crise, les plans de reprise d'activité (PRA) et les plans de continuité d'activité (PCA) à mettre en place pour assurer la résilience des SIE en cas d'incident majeur.
- **La conformité réglementaire et normative** : intégrant les exigences du cadre juridique et réglementaire applicable à la sécurité numérique, ainsi que les référentiels de bonnes pratiques et les normes de sécurité (ISO 27001, etc.).

La PSSIE est un document évolutif, régulièrement mis à jour pour tenir compte de l'évolution des menaces, des technologies et des bonnes pratiques en matière de cybersécurité. Elle constitue le socle commun de la sécurité numérique de l'État, et sa mise en œuvre effective est un enjeu majeur pour la protection des intérêts de la nation et la confiance des citoyens dans les services publics numériques.

1.5.3. En résume

La protection des systèmes d'information de l'État est un domaine spécifique et crucial du cadre réglementaire français de la SSI. Le décret n° 2022-513 et la PSSIE constituent les textes de référence qui définissent la gouvernance, les principes et les exigences de sécurité applicables à l'ensemble de l'administration publique. Ces textes visent à garantir un niveau élevé de cybersécurité pour les SIE, à renforcer la résilience de l'État face aux cybermenaces et à assurer la continuité des services publics numériques.

1.6. La détection

La détection des événements susceptibles d'affecter la sécurité des systèmes d'information est un pilier essentiel d'une stratégie de cybersécurité efficace. La capacité à détecter rapidement les incidents, les vulnérabilités et les menaces permet de réagir promptement, de limiter les dommages et de restaurer la situation normale dans les meilleurs délais. Le cadre réglementaire français de la SSI reconnaît l'importance de la détection et encadre les dispositifs et les mécanismes mis en œuvre à cette fin, en particulier en ce qui concerne les opérateurs de communications électroniques (OCE) et les prérogatives de l'ANSSI.

Les deux articles de loi clés relatifs à la détection sont :

1.6.1. L'Article L.33-14 du code des postes et communications électroniques (CPCE) :

Cet article du CPCE encadre la possibilité pour les opérateurs de communications électroniques (OCE) de mettre en œuvre des dispositifs de détection des événements

susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés. Il définit également le cadre permettant à l'ANSSI de s'appuyer sur ces capacités de détection.

- **Objectifs et portée :** L'article L.33-14 du CPCE vise à encourager et à encadrer la mise en place de dispositifs de détection par les OCE, qui sont des acteurs clés de l'infrastructure numérique et disposent d'une position privilégiée pour observer le trafic et les événements sur leurs réseaux. Il a un double objectif :
    - **Permettre aux OCE d'améliorer la sécurité de leurs propres systèmes d'information et de ceux de leurs abonnés** : en détectant les menaces et les incidents et en prenant les mesures appropriées pour les prévenir ou les atténuer.
    - **Fournir à l'ANSSI des capacités de détection supplémentaires** : en permettant à l'ANSSI de s'appuyer sur les dispositifs de détection mis en œuvre par les OCE pour surveiller l'état de la cybersécurité au niveau national et détecter les menaces potentielles.
- **Principales dispositions :** L'article L.33-14 du CPCE prévoit plusieurs dispositions importantes :
    - **L'autorisation pour les OCE de mettre en œuvre des dispositifs de détection** : sous réserve du respect des dispositions légales relatives à la protection des données personnelles et au secret des correspondances. Les OCE doivent notamment informer leurs abonnés de la mise en place de ces dispositifs et garantir le respect de leur vie privée.
    - **La possibilité pour l'ANSSI de s'appuyer sur les capacités de détection des OCE** : dans le cadre de ses missions de surveillance et de défense des systèmes d'information. L'ANSSI peut notamment demander aux OCE de lui transmettre des informations agrégées ou anonymisées sur les événements de sécurité détectés, ou de mettre en œuvre des dispositifs de détection spécifiques à sa demande.
    - **L'obligation pour les OCE de transmettre des messages de signalement de vulnérabilité ou de suspicion de compromission auprès de leurs abonnés** : à la demande de l'ANSSI. Cela permet à l'ANSSI d'alerter rapidement les abonnés des OCE en cas de vulnérabilité détectée sur leurs systèmes d'information ou de suspicion de compromission, et de leur fournir des recommandations pour y remédier. Cette disposition vise à renforcer la réactivité face aux menaces et à améliorer la sécurité des systèmes d'information des abonnés des OCE.

L'article L.33-14 du CPCE constitue un instrument important pour renforcer les capacités de détection des incidents de sécurité en France, en s'appuyant sur l'expertise et les infrastructures des opérateurs de communications électroniques, tout en encadrant strictement l'utilisation de ces dispositifs pour garantir le respect des libertés individuelles.

1.6.2. L'Article L. 2321-2-1 du code de la défense :

Cet article du code de la défense autorise l'ANSSI à déployer à des fins de caractérisation de la menace, un dispositif de détection sur le réseau d'un opérateur de communications électroniques ou sur le système d'information d'un fournisseur d'accès ou d'un hébergeur. Il confère à l'ANSSI des prérogatives spécifiques pour mener des actions de détection proactive et d'analyse de la menace cybernétique.

- **Objectifs et portée :** L'article L. 2321-2-1 du code de la défense vise à donner à l'ANSSI les moyens juridiques de mener des actions de détection proactive et d'analyse de la menace cybernétique, afin de mieux comprendre les modes opératoires des attaquants, d'anticiper les attaques et de renforcer la défense des systèmes d'information. Il s'inscrit dans une logique de défense active et de renseignement cybernétique. Il autorise l'ANSSI à déployer des dispositifs de détection non seulement sur les réseaux des OCE, mais aussi sur les systèmes d'information des fournisseurs d'accès internet (FAI) et des hébergeurs, élargissant ainsi son champ d'action.
- **Principales dispositions :** L'article L. 2321-2-1 du code de la défense prévoit :
    - **L'autorisation pour l'ANSSI de déployer des dispositifs de détection** : sur les réseaux des OCE, les systèmes d'information des FAI et des hébergeurs. Ce déploiement est soumis à certaines conditions et garanties, notamment en termes de finalité (caractérisation de la menace) et de durée limitée.
    - **La finalité du déploiement des dispositifs de détection** : est strictement limitée à la caractérisation de la menace cybernétique. Il ne s'agit pas de surveiller les communications des utilisateurs, mais de collecter des informations techniques sur les attaques, les vulnérabilités et les modes opératoires des attaquants.
    - **Le cadre juridique et les garanties** : le déploiement de ces dispositifs est encadré par des procédures strictes et soumis au contrôle de la Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR). Des garanties sont prévues pour protéger la vie privée des personnes et le secret des correspondances.

L'article L. 2321-2-1 du code de la défense confère à l'ANSSI des capacités importantes pour mener des actions de renseignement cybernétique et améliorer sa connaissance de la menace. Il permet à l'ANSSI de jouer un rôle plus proactif dans la défense des systèmes d'information, en allant au-delà de la simple réponse aux incidents et en anticipant les attaques potentielles.

1.6.3. En résumé

La détection des incidents de sécurité est une composante essentielle du cadre réglementaire français de la SSI. L'article L.33-14 du CPCE et l'article L. 2321-2-1 du code de la défense définissent le cadre juridique permettant aux OCE de mettre en œuvre des dispositifs de détection et confèrent à l'ANSSI des prérogatives spécifiques pour s'appuyer sur ces capacités et pour mener des actions de détection proactive et d'analyse de la menace. Ces dispositions

visent à renforcer la capacité de la France à détecter rapidement les incidents de sécurité, à comprendre les menaces et à y répondre efficacement.

partie 2: Le Cadre Réglementaire de la Confiance Numérique

2.1. Introduction au Cadre Réglementaire de la Confiance Numérique

La transformation numérique de la société, qui se caractérise certes par la dématérialisation croissante des échanges et des services, révèle les besoins d'un cyberespace de confiance. La confiance numérique ne se limite pas à la seule sécurité des systèmes d'information. C'est un ensemble de mesures et de réglementations, dont l'objectif est d'assurer la sécurité technique des infrastructures numériques, la fiabilité des données échangées, la sécurité des services mis en œuvre, et enfin le respect des droits des personnes. La sécurité des systèmes d'information vise à répondre aux enjeux de protection des actifs numériques et à lutter contre les cyberattaques, la confiance numérique a pour objectif de créer un environnement numérique rassurant qui permet aux utilisateurs d'interagir, d'échanger, et de réaliser des transactions en toute quiétude. Elle repose sur la mise en place de mécanismes de certification, d'identification électronique, de protection des données personnelles, et de contrôle des technologies pouvant porter atteinte à la vie privée.

Tel qu'il a été mis en avant dans le texte d'ouverture, l'ANSSI est un acteur remarquable dans l'édification de ce cyberespace de confiance. En effet, elle participe à la vérification de la sécurité des dispositifs techniques en œuvre, à l'évaluation de la fiabilité des offreurs de services en cybersécurité, au contrôle de la diffusion des moyens de cryptologie, à la surveillance de la mise en œuvre des dispositifs susceptibles d'atteindre à l'intimité. En somme, l'ANSSI est garante d'une confiance numérique et amène les acteurs à adopter des pratiques plus respectueuses des droits fondamentaux, tout en étant plus sûres.

Le cadre réglementaire de la confiance numérique peut être structuré en quatre grandes catégories, permettant une approche ciblée et sectorielle :

1. **La sécurité des échanges par voie électronique** : Concerne les réglementations visant à sécuriser les échanges numériques entre les administrations, les entreprises et les citoyens, en garantissant l'intégrité, la confidentialité et la non-répudiation des informations échangées.
2. **Le cadre de certification de cybersécurité européen** : S'inscrit dans une démarche d'harmonisation européenne visant à établir un cadre commun pour la certification de cybersécurité des produits, services et processus numériques, afin de renforcer la confiance dans le marché unique numérique.
3. **Les contrôles réglementaires sur la cryptographie** : Visent à encadrer l'utilisation et la diffusion des moyens de cryptologie, qui sont à la fois des outils essentiels pour la sécurité numérique et des technologies potentiellement sensibles nécessitant un contrôle réglementaire.
4. **La protection de la vie privée et du secret des correspondances** : Concerne les réglementations visant à protéger la vie privée des citoyens dans l'environnement

numérique, en encadrant l'utilisation des technologies pouvant porter atteinte à la vie privée et au secret des correspondances.

2.2. La sécurité des échanges par voie électronique

La sécurité des échanges par voie électronique est un pilier fondamental de la confiance numérique. Dans un monde où les interactions numériques se multiplient, il est essentiel de garantir la sécurité, la fiabilité et la légalité de ces échanges, qu'ils aient lieu entre les administrations, entre les entreprises, ou entre les administrations et les citoyens. Le cadre réglementaire français, en cohérence avec les initiatives européennes, a mis en place plusieurs dispositifs pour sécuriser ces échanges.

Les trois éléments réglementaires clés dans ce domaine :

2.2.1. Le Référentiel Général de Sécurité (RGS) :

Le RGS est un référentiel normatif français qui impose aux autorités administratives françaises des règles de cybersécurité pour leurs échanges par voie électronique avec d'autres administrations et avec les citoyens. Il définit également les exigences applicables aux produits et services de confiance utilisés dans le cadre de ces échanges. Le RGS est un outil essentiel pour garantir la sécurité et l'interopérabilité des échanges numériques au sein de l'administration publique et avec les usagers.

- **Objectifs et portée :** L'objectif principal du RGS est de renforcer la sécurité des échanges électroniques des autorités administratives françaises, en définissant un cadre de référence pour la mise en œuvre de mesures de sécurité adaptées aux risques. Il vise à garantir la confidentialité, l'intégrité, la disponibilité et la non-répudiation des informations échangées. Le RGS s'applique à toutes les autorités administratives françaises, centrales et déconcentrées, ainsi qu'aux établissements publics administratifs. Il couvre un large éventail d'échanges électroniques, tels que les démarches administratives en ligne, les échanges de courriers électroniques, les téléservices, les systèmes d'information inter-administrations, etc.
- **Principales exigences :** Le RGS définit un ensemble d'exigences organisationnelles et techniques pour la sécurité des échanges électroniques. Parmi les exigences organisationnelles, on retrouve la désignation d'un responsable de la sécurité des systèmes d'information (RSSI), la mise en place d'une politique de sécurité, la gestion des risques, la sensibilisation et la formation du personnel, la gestion des identités et des accès, la gestion des incidents de sécurité et la mise en place de plans de continuité d'activité (PCA). Parmi les exigences techniques, le RGS couvre un large spectre de domaines, tels que l'authentification forte, la signature électronique, le chiffrement des données, la journalisation et l'audit de sécurité, la sécurité des réseaux, des systèmes et des applications, la protection contre les intrusions et les logiciels malveillants, etc. Le RGS

distingue différents niveaux de sécurité (standard, renforcé, élevé) en fonction des risques et des enjeux associés aux échanges électroniques. Il impose également des exigences spécifiques pour les produits et services de confiance utilisés dans les échanges électroniques, tels que les certificats électroniques, les horodatages qualifiés, les services de signature électronique, etc. Le RGS est régulièrement mis à jour pour tenir compte de l'évolution des menaces et des technologies.

2.2.2. Le Règlement européen n°910/2014 « eIDAS » :

Le règlement eIDAS (electronic IDentification, Authentication and trust Services) est un règlement européen qui définit au niveau européen les exigences applicables en matière d'identification électronique ainsi qu'aux prestataires de services de confiance, ainsi que les effets juridiques et modalités de reconnaissance mutuelle. eIDAS vise à créer un marché unique numérique de confiance en facilitant la reconnaissance mutuelle et l'acceptation transfrontalière des moyens d'identification électronique et des services de confiance dans l'ensemble de l'UE.

- **Objectifs et portée :** L'objectif principal du règlement eIDAS est de renforcer la confiance dans les transactions électroniques au sein de l'Union européenne, en créant un cadre juridique harmonisé pour l'identification électronique et les services de confiance. Il vise à faciliter les échanges transfrontaliers, à stimuler le commerce électronique et à améliorer l'efficacité des services publics numériques. Le règlement eIDAS s'applique à tous les États membres de l'UE et concerne :
    - **L'identification électronique (eID)** : il établit un cadre pour la reconnaissance mutuelle des systèmes d'identification électronique nationaux, permettant aux citoyens et aux entreprises d'utiliser leur identité numérique nationale pour accéder à des services en ligne dans d'autres États membres. Il définit différents niveaux d'assurance pour l'identification électronique (faible, substantiel, élevé).
    - **Les services de confiance** : il définit un cadre juridique pour les services de confiance, tels que les certificats électroniques, les horodatages qualifiés, les services d'envoi recommandé électronique, les services de signature électronique et les services de validation des signatures électroniques. Il établit des exigences pour les prestataires de services de confiance qualifiés et pour les services de confiance qualifiés, qui bénéficient d'une reconnaissance juridique renforcée dans l'ensemble de l'UE.
- **Principales exigences :** Le règlement eIDAS impose aux États membres de :
    - Reconnaître mutuellement les systèmes d'identification électronique notifiés par d'autres États membres, sous certaines conditions.
    - Mettre en place un cadre national pour la supervision des prestataires de services de confiance et pour la délivrance du statut de prestataire de services de confiance qualifié.

- Adopter des règles nationales pour la responsabilité des prestataires de services de confiance.
- Coopérer avec les autres États membres et avec la Commission européenne pour la mise en œuvre du règlement eIDAS.

Le règlement eIDAS est un texte fondamental pour la construction d'un marché unique numérique de confiance en Europe. Il facilite les échanges transfrontaliers, renforce la sécurité juridique des transactions électroniques et stimule l'innovation dans le domaine des services de confiance.

2.2.3. Les articles L.100 à L.103 du code des postes et communications électroniques (CPCE) :

Ces articles du CPCE définissent au niveau national les exigences et les modalités de certification relatives aux services introduits par la loi pour une République numérique : l'identification électronique, les coffres-forts numériques et la lettre recommandée électronique. Ils complètent le règlement eIDAS en précisant le cadre juridique national pour certains services de confiance spécifiques.

- **Objectifs et portée :** Les articles L.100 à L.103 du CPCE visent à transposer et à compléter le règlement eIDAS en droit français, en définissant un cadre juridique national pour certains services de confiance qui ont été introduits ou renforcés par la loi pour une République numérique du 7 octobre 2016. Ils concernent principalement :
  - **L'identification électronique** : en précisant les modalités de certification des dispositifs d'identification électronique et en reconnaissant la valeur juridique de l'identification électronique qualifiée.
  - **Les coffres-forts numériques** : en définissant un cadre juridique pour les services de coffre-fort numérique, permettant aux utilisateurs de stocker et de gérer des documents numériques de manière sécurisée et confidentielle, avec une valeur probante.
  - **La lettre recommandée électronique** : en définissant un cadre juridique pour la lettre recommandée électronique, qui bénéficie de la même valeur juridique que la lettre recommandée papier, sous certaines conditions.
- **Principales exigences :** Les articles L.100 à L.103 du CPCE définissent :
  - Les exigences de certification pour les prestataires de services de confiance offrant des services d'identification électronique, de coffre-fort numérique et de lettre recommandée électronique. Ces exigences portent notamment sur la sécurité, la fiabilité, la qualité de service et la protection des données personnelles.
  - Les modalités de reconnaissance juridique des services de confiance certifiés.
  - Les règles relatives à la responsabilité des prestataires de services de confiance.

- Les pouvoirs de contrôle et de sanction de l'autorité compétente (l'ANSSI en général, ou d'autres autorités sectorielles pour certains services spécifiques).

Les articles L.100 à L.103 du CPCE contribuent à renforcer le cadre juridique français pour la confiance numérique, en précisant les règles applicables à des services de confiance spécifiques et en favorisant leur développement et leur adoption.

2.2.4. En résumé

La sécurité des échanges par voie électronique en France repose sur un cadre réglementaire solide, articulé autour du RGS pour les administrations publiques, du règlement eIDAS au niveau européen, et des articles L.100 à L.103 du CPCE au niveau national pour certains services de confiance spécifiques. Ces dispositifs visent à garantir la sécurité, la fiabilité et la légalité des échanges numériques, en favorisant la confiance des utilisateurs et en stimulant le développement de l'économie numérique.

2.3. Le cadre de certification de cybersécurité européen

2.3.1. Le règlement européen n° 2019/881 « Cybersecurity Act »

Le règlement européen n° 2019/881 relatif à la cybersécurité (appelé « Cybersecurity Act ») constitue un axe fort du cadre européen de confiance numérique. Il a pour objet de définir un cadre de certification de cybersécurité des produits, services et processus liés aux technologies de l'information, harmonisé à l'échelle européenne. Le Cybersecurity Act a pour but de « renforcer la cybersécurité dans l'union européenne en établissant un système de certification commun, afin d'augmenter la confiance des utilisateurs, consommateurs et entreprises dans les produits et services numériques ».

- **Objectifs et portée :** L'objectif principal du Cybersecurity Act est de créer un cadre européen de certification de cybersécurité pour les produits, services et processus des technologies de l'information et de la communication (TIC). Il vise à :
    - **Accroître le niveau de cybersécurité des produits et services numériques disponibles sur le marché européen** : en encourageant les fabricants et les fournisseurs à intégrer la sécurité dès la conception et à se soumettre à des schémas de certification.
    - **Renforcer la confiance des consommateurs, des entreprises et des administrations publiques dans les produits et services numériques** : en leur fournissant des informations claires et fiables sur le niveau de cybersécurité des produits et services certifiés.

- **Faciliter le commerce transfrontalier des produits et services numériques certifiés** : en assurant la reconnaissance mutuelle des certificats de cybersécurité dans l'ensemble de l'UE, et en évitant la fragmentation du marché intérieur.
- **Promouvoir une culture de la cybersécurité au sein de l'Union européenne**.

La portée du Cybersecurity Act couvre un large éventail de produits, de services et de processus TIC, qu'il s'agisse d'équipements informatiques, de logiciels, d'infrastructures numériques, de services cloud, d'objets connectés, etc. Il ne vise pas à dresser une liste renouvelable de produits et de services concernés, mais plutôt à imposer un cadre global qui sera éventuellement adapté aux différents secteurs et catégories de produits et de services.

- **Principales dispositions et mécanismes :** Le Cybersecurity Act met en place plusieurs mécanismes clés pour atteindre ses objectifs :
  - **L'établissement d'un cadre européen de certification de cybersécurité** : Le règlement définit les principes généraux et les règles de base pour l'élaboration de **schémas de certification de cybersécurité européens**. Ces schémas de certification sont élaborés par l'ENISA (Agence de l'Union européenne pour la cybersécurité), en coopération avec les États membres et les parties prenantes (industries, organisations de consommateurs, etc.). Chaque schéma de certification définit :
    - **Le ou les catégories de produits, services et processus TIC concernés**.
    - **Les exigences de cybersécurité** auxquelles doivent satisfaire les produits, services ou processus pour obtenir la certification. Ces exigences peuvent porter sur différents aspects de la sécurité, tels que la sécurité des fonctionnalités, la sécurité des données, la résistance aux attaques, la gestion des vulnérabilités, etc.
    - **Les niveaux d'assurance** de la certification (de base, substantiel, élevé), correspondant à des niveaux de rigueur et de contrôle croissants.
    - **Les procédures d'évaluation de la conformité** (auto-évaluation, évaluation par un organisme tiers, etc.) et de délivrance des certificats.
    - **Les modalités de surveillance et de renouvellement des certificats**.
  - **La création d'un Comité européen de certification de cybersécurité (ECCG)** : Le ECCG est composé de représentants des autorités nationales de certification de cybersécurité des États membres. Il a pour mission de conseiller et d'assister la Commission européenne et l'ENISA dans l'élaboration et la mise en œuvre des schémas de certification européens, de coordonner les politiques nationales de certification, et de garantir la cohérence et l'harmonisation du système de certification à l'échelle de l'UE.
  - **La désignation d'autorités nationales de certification de cybersécurité (ANCC)** : Chaque État membre doit désigner une ou plusieurs ANCC, chargées de mettre en œuvre le cadre de certification européen au niveau national. Les ANCC sont responsables de l'accréditation des organismes d'évaluation de la conformité, de la surveillance du marché des produits et services certifiés, et de la coopération avec les

autres ANCC et avec l'ENISA. En France, l'ANSSI est l'autorité nationale de certification de cybersécurité.

- **La reconnaissance mutuelle des certificats de cybersécurité européens** : Les certificats de cybersécurité délivrés dans le cadre d'un schéma de certification européen sont valables et reconnus dans tous les États membres de l'UE. Cela facilite le commerce transfrontalier et réduit les coûts de certification pour les entreprises opérant dans plusieurs États membres.
- **Le volontariat de la certification (en principe)** : En principe, la certification de cybersécurité est volontaire pour les fabricants et les fournisseurs de produits et services TIC. Cependant, le Cybersecurity Act prévoit la possibilité d'introduire des schémas de certification obligatoires pour certaines catégories de produits et services, notamment dans des secteurs critiques ou à haut risque. De plus, la certification peut devenir de facto obligatoire pour accéder à certains marchés publics ou privés, ou pour se conformer à d'autres réglementations (par exemple, le RGPD).

Le Cybersecurity Act marque l'étape décisive d'une volonté d'y parvenir, en ce sens qu'il vise à construire un véritable écosystème de confiance dans lequel les consommateurs, les entreprises sont assurés de bénéficier de produits et de services numériques évalués et certifiés selon des normes de sécurité élevées. La mise en œuvre et l'adoption par le marché des schémas de certification européens constitueront un facteur déterminant du succès de ce règlement.

2.3.2. En résumé

le Cybersecurity Act établit un cadre européen de certification de cybersécurité harmonisé, basé sur des schémas de certification élaborés par l'ENISA et mis en œuvre par les autorités nationales de certification. Il vise à renforcer la confiance dans les produits et services numériques, à faciliter le commerce transfrontalier et à promouvoir une culture de la cybersécurité au sein de l'Union européenne.

2.4. Les contrôles réglementaires sur la cryptographie

La cryptographie revêt une importance capitale en matière de sécurité des systèmes d'information et de confiance numérique. En effet, elle permet d'assurer la confidentialité, l'intégrité et l'authenticité des informations et communications numériques. Il est nécessaire, cependant, de la contrôler car elle pourrait servir à des fins illicites ou malveillantes, ce qui a conduit à des mécanismes réglementaires au niveau national et européen visant à garantir simultanément l'usage de la cryptographie pour sécuriser le numérique et prévenir les usages abusifs.

Les trois textes réglementaires clés dans ce domaine :

2.4.1. La Loi n°2004-575 du 21 juin 2004 (LCEN) et le Décret 2007-663 du 2 mai 2007 :

La loi LCEN (Loi pour la Confiance dans l'Économie Numérique) et le décret d'application n° 2007-663 du 2 mai 2007 définissent **les modalités de contrôle domestique (fourniture, importation, transfert intracommunautaire et exportation) des moyens de cryptologie** en France. Ce cadre réglementaire national vise à encadrer l'utilisation et la diffusion des moyens de cryptologie sur le territoire français.

- **Objectifs et portée :** L'objectif principal de la réglementation française sur la cryptographie est de concilier deux impératifs :
    - **Faciliter l'utilisation de la cryptographie pour la protection des données et des communications numériques** : reconnaissant son rôle essentiel pour la sécurité et la confiance dans l'économie numérique.
    - **Prévenir l'utilisation abusive de la cryptographie à des fins illégales ou malveillantes** : telles que le terrorisme, la criminalité organisée, l'atteinte aux intérêts fondamentaux de la nation, etc.

La réglementation française concernant la cryptographie porte sur les moyens de cryptologie, entendus comme les matériels ou logiciels conçus ou modifiés pour réaliser la transformation de données en vue de garantir leur confidentialité ou leur authentification ou encore leur intégrité. Un vaste type d'opérations est régi par la réglementation sur les moyens de cryptologie : fourniture, importation, transfert intracommunautaire, exportation et, dans certains cas, détention ou utilisation.

- **Principales dispositions et mécanismes :** La réglementation française sur la cryptographie distingue deux régimes principaux de contrôle, en fonction de la nature des moyens de cryptologie :
    - **Le régime de la déclaration** : Concerne les **moyens de cryptologie dits "en clair" ou "grand public"**, qui sont principalement destinés à des fonctions d'authentification ou de contrôle d'intégrité, ou qui mettent en œuvre des algorithmes de chiffrement considérés comme peu sensibles. Pour ces moyens de cryptologie, la fourniture, l'importation et le transfert intracommunautaire sont soumis à une simple **déclaration préalable** auprès de l'ANSSI. L'exportation reste soumise à un régime d'autorisation (voir ci-dessous).
    - **Le régime de l'autorisation** : Concerne les **moyens de cryptologie dits "de sécurité" ou "sensibles"**, qui mettent en œuvre des algorithmes de chiffrement robustes et qui sont principalement destinés à des fonctions de confidentialité. Pour ces moyens de cryptologie, la fourniture, l'importation, le transfert intracommunautaire et l'exportation sont soumis à une **autorisation préalable** de l'ANSSI. L'autorisation est délivrée après examen de la demande, en tenant compte de différents critères, tels que la nature du moyen de cryptologie, son usage prévu, les garanties de sécurité offertes, etc.

Le décret n° 2007-663 spécifie les catégories de moyens de cryptologie soumis à déclaration et à autorisation, ainsi que les modalités de déclaration et de demande d'autorisation. L'ANSSI est l'autorité compétente pour la gestion de ces contrôles et la délivrance des autorisations. La réglementation française en matière de cryptologie est régulièrement mise à jour pour tenir compte de l'évolution des techniques et des menaces, afin de rechercher un équilibre entre la promotion de la cryptologie et la lutte contre son utilisation malveillante.

2.4.2. Le Règlement délégué (UE) 2019/2199 de la Commission européenne :

Ce règlement délégué de la Commission européenne **définit au niveau européen les modalités de contrôle d'export des moyens de cryptologie**. Il s'inscrit dans le cadre du règlement (CE) n° 428/2009 du Conseil instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage. Ce règlement européen vise à harmoniser et à renforcer les contrôles à l'exportation des moyens de cryptologie au sein de l'Union européenne.

- **Objectifs et portée :** L'objectif principal du règlement délégué (UE) 2019/2199 est d'encadrer les exportations de moyens de cryptologie depuis l'Union européenne vers les pays tiers, afin de prévenir la prolifération de technologies sensibles et de garantir la sécurité internationale. Il vise à :
    - **Harmoniser les contrôles à l'exportation des moyens de cryptologie au sein de l'UE** : en définissant des règles communes et des listes de contrôle harmonisées.
    - **Renforcer l'efficacité des contrôles à l'exportation** : en améliorant la coopération entre les États membres et en mettant en place des mécanismes de suivi et d'échange d'informations.
    - **Prévenir la prolifération des technologies de cryptographie les plus sensibles** : vers des pays ou des entités présentant des risques pour la sécurité internationale, les droits de l'homme ou les intérêts de l'UE.

Le règlement délégué (UE) 2019/2199 s'applique à l'exportation de biens à double usage relevant de la catégorie 5 de l'annexe I du règlement (CE) n° 428/2009, qui comprend notamment les moyens de cryptologie. Il définit des listes de contrôle spécifiques pour les différents types de moyens de cryptologie, en fonction de leur sensibilité et de leur potentiel d'usage militaire ou de sécurité.

- **Principales dispositions et mécanismes :** Le règlement délégué (UE) 2019/2199 met en place plusieurs mécanismes clés pour le contrôle des exportations de cryptographie :
    - **L'établissement de listes de contrôle harmonisées au niveau européen** : Ces listes définissent les catégories de moyens de cryptologie soumises à autorisation d'exportation, en fonction de leur niveau de sensibilité et de leur destination. Les listes de contrôle sont régulièrement mises à jour pour tenir compte de l'évolution des technologies et des enjeux géopolitiques.

- **La mise en place d'un système d'autorisations d'exportation** : L'exportation des moyens de cryptologie figurant sur les listes de contrôle est soumise à une autorisation préalable délivrée par les autorités compétentes des États membres (en France, le Service des biens à double usage - SBDU, rattaché au Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique). Les autorités compétentes examinent les demandes d'autorisation en tenant compte de différents critères, tels que la nature du moyen de cryptologie, sa destination, son utilisateur final, son usage prévu, les risques de détournement, etc.
- **La coopération et l'échange d'informations entre les États membres** : Le règlement prévoit des mécanismes de coopération et d'échange d'informations entre les autorités compétentes des États membres, afin d'assurer une application cohérente et efficace des contrôles à l'exportation, et de prévenir les risques de contournement des contrôles.
- **Des dispositions spécifiques pour certains types d'exportations** : Le règlement prévoit des dispositions spécifiques pour les exportations vers certains pays, pour les exportations de technologies de cryptographie à code source ouvert, ou pour les exportations à des fins de recherche scientifique.

Le règlement délégué (UE) 2019/2199 vise à renforcer et à mieux coordonner la régulation des exportations de cryptographie au niveau européen, et à prévenir la prolifération des technologies sensibles, dans un cadre global de l'Union européenne visant également à garantir la sécurité internationale et à promouvoir un usage responsable des technologies de cryptographie.

2.4.3. En résumé

Les contrôles réglementaires en matière de cryptographie dans la France et dans l'Union européenne visent à trouver un équilibre précaire entre la promotion de l'utilisation de la cryptographie pour la sécurité numérique, et la prévention de son utilisation malveillante. La réglementation française (LCEN et décret 2007-663) ne concerne que les opérations domestiques sur les moyens de cryptologie (fourniture, importation, transfert intracommunautaire), tandis que le règlement délégué (rég CE 2019/2199) vise à renforcer et harmoniser les contrôles à l'exportation des moyens de cryptologie depuis l'Union européenne. La mise en place de ce cadre de régulation, en synergie avec d'autres modalités réglementaires et le respect des bonnes pratiques, est essentielle pour garantir un usage responsable et sécurisé de la cryptographie dans un environnement numérique de plus en plus risquer et incertain.

2.5. La protection de la vie privée et du secret des correspondances

La protection de la vie privée et du secret des correspondances est un droit fondamental reconnu et garanti en France, y compris dans l'environnement numérique. Le cadre réglementaire français de la confiance numérique intègre des dispositions spécifiques visant à protéger ces droits face aux risques liés aux technologies numériques, notamment en encadrant l'utilisation de dispositifs techniques susceptibles de porter atteinte à la vie privée et au secret des communications.

Les deux textes réglementaires clés dans ce domaine :

2.5.1. Les articles R.226-1 et suivants du code pénal :

Ces articles du code pénal définissent le cadre réglementaire applicable aux appareils ou dispositifs techniques pouvant porter atteinte au respect de la vie privée et au secret des correspondances. Ils incriminent notamment certaines actions portant atteinte à ces droits fondamentaux, en particulier lorsqu'elles sont réalisées au moyen de dispositifs techniques spécifiques.

- **Objectifs et portée :** L'objectif principal des articles R.226-1 et suivants du code pénal est de protéger la vie privée des personnes et le secret de leurs correspondances contre les atteintes illégales, en particulier celles qui sont facilitées ou rendues possibles par l'utilisation de technologies intrusives. Ils visent à :
    - **Réprimer les atteintes à la vie privée** : telles que la captation, l'enregistrement ou la diffusion sans consentement d'images, de paroles ou de données à caractère personnel relevant de la vie privée.
    - **Réprimer les atteintes au secret des correspondances** : telles que l'interception, la divulgation ou l'utilisation non autorisée de correspondances émises, reçues ou détenues par des tiers.
    - **Encadrer l'utilisation de dispositifs techniques susceptibles de porter atteinte à ces droits** : en incriminant certaines actions réalisées au moyen de ces dispositifs, et en prévoyant des sanctions pénales pour les infractions.

Les articles R.226-1 et suivants du code pénal s'appliquent à un large éventail de situations et de dispositifs techniques susceptibles de porter atteinte à la vie privée et au secret des correspondances tel que :

- **Les appareils de captation ou d'enregistrement clandestin** : microphones cachés, caméras espions, enregistreurs audio ou vidéo dissimulés, etc.
- **Les logiciels espions (spyware)** : programmes informatiques conçus pour surveiller à distance l'activité d'un ordinateur ou d'un téléphone, collecter des données personnelles, intercepter des communications, etc.

- **Les dispositifs de géolocalisation** : balises GPS, applications de suivi de localisation, etc., lorsqu'ils sont utilisés pour surveiller les déplacements d'une personne sans son consentement.
- **Les dispositifs d'intrusion dans les systèmes informatiques** : logiciels de piratage, outils de surveillance réseau, etc., lorsqu'ils sont utilisés pour accéder illégalement à des données personnelles ou à des correspondances.

- **Principales incriminations et sanctions :** Les articles R.226-1 et suivants du code pénal incriminent plusieurs types d'infractions, en fonction de la nature de l'atteinte et des moyens utilisés :
  - **L'atteinte à l'intimité de la vie privée par captation, enregistrement ou transmission de paroles ou d'images** (article 226-1 du code pénal) : est punie d'un an d'emprisonnement et de 45 000 euros d'amende. Cette infraction vise notamment l'utilisation de dispositifs de captation clandestins pour enregistrer ou transmettre des conversations privées ou des images relevant de la vie privée.
  - **L'atteinte au secret des correspondances** (article 226-15 du code pénal) : est punie d'un an d'emprisonnement et de 45 000 euros d'amende. Cette infraction vise notamment l'interception, la divulgation ou l'utilisation non autorisée de correspondances émises, reçues ou détenues par des tiers, quel que soit le support utilisé (papier, électronique, etc.).
  - **La fabrication, l'importation, la détention, la cession, la publicité ou la commercialisation d'appareils ou de dispositifs techniques spécialement conçus pour réaliser les infractions précédentes** (article 226-20 du code pénal) : est également punie d'un an d'emprisonnement et de 45 000 euros d'amende. Cette infraction vise à encadrer la diffusion et la disponibilité des dispositifs techniques intrinsèquement conçus pour porter atteinte à la vie privée et au secret des correspondances.

Les articles R.226-1 et suivants du code pénal constituent un socle juridique important pour la protection de la vie privée et du secret des correspondances dans le droit français, en incriminant les atteintes les plus graves et en prévoyant des sanctions pénales dissuasives.

2.5.2. L'arrêté du 4 juillet 2012 :

Cet arrêté liste en annexe les appareils ou dispositifs techniques mentionnés à l'article 226-20 du code pénal, dont la fabrication, l'importation, la détention, la cession, la publicité ou la commercialisation sont spécifiquement incriminées. L'arrêté du 4 juillet 2012 précise et actualise la liste des dispositifs techniques considérés comme particulièrement intrusifs et susceptibles de porter atteinte à la vie privée et au secret des correspondances.

- **Objectifs et portée :** L'objectif de l'arrêté du 4 juillet 2012 est de donner une portée concrète à l'article 226-20 du code pénal, en identifiant de manière précise les types d'appareils ou de dispositifs techniques dont la diffusion et l'utilisation doivent être particulièrement encadrées en raison de leur potentiel intrusif. Il vise à :

- **Clarifier le champ d'application de l'article 226-20 du code pénal** : en fournissant une liste indicative, mais non exhaustive, des dispositifs techniques concernés.
- **Sensibiliser les acteurs économiques et les utilisateurs** : sur les risques d'atteinte à la vie privée et au secret des correspondances liés à certains dispositifs techniques.
- **Faciliter l'action des forces de l'ordre et de la justice** : dans la lutte contre la diffusion et l'utilisation illégales de ces dispositifs.

- **Contenu de l'annexe de l'arrêté du 4 juillet 2012 :** L'annexe de l'arrêté du 4 juillet 2012 liste plusieurs catégories d'appareils ou de dispositifs techniques, classés en fonction de leur fonction principale :
  - **Appareils de captation de sons ou de paroles** : microphones miniatures, micros espions, appareils d'enregistrement dissimulés, etc.
  - **Appareils de prise de vue ou de vidéo** : mini-caméras, caméras espions, lunettes ou stylos caméra, etc.
  - **Appareils de localisation** : balises GPS, traceurs GPS, applications de suivi de localisation spécialement conçues pour la surveillance, etc.
  - **Logiciels de surveillance** : spyware, keyloggers, outils de surveillance à distance, etc., spécialement conçus pour intercepter des communications, collecter des données personnelles ou surveiller l'activité d'un système informatique.
  - **Dispositifs de brouillage ou de neutralisation de systèmes de sécurité** : lorsqu'ils sont spécifiquement conçus pour faciliter l'atteinte à la vie privée ou au secret des correspondances.

La liste de l'annexe de l'arrêté du 4 juillet 2012 n'est pas exhaustive et peut être mise à jour pour tenir compte de l'évolution des technologies et des pratiques intrusives. Elle constitue un outil utile pour l'interprétation et l'application de l'article 226-20 du code pénal, et pour la sensibilisation aux risques d'atteinte à la vie privée et au secret des correspondances liés à certains dispositifs techniques.

2.5.3. En résumé

La protection de la vie privée et du secret des correspondances dans le cadre de la confiance numérique repose sur un cadre juridique et réglementaire incriminant les atteintes à ces droits fondamentaux, notamment lorsque celles-ci sont réalisées au moyen de dispositifs techniques déterminés. Les articles R.226-1 et suivants du code pénal répriment les infractions et fixent les sanctions applicables, alors que l'arrêté du 4 juillet 2012 détermine la liste des appareils ou dispositifs techniques particulièrement visés. Ces dispositions délocalisées visent à garantir le respect de la vie privée et du secret des communications dans l'environnement numérique, en réglementant l'usage de technologies potentiellement intrusives.

partie 3 : Application Pratique Un Chatbot IA pour la Consultation du Cadre Réglementaire

L'étendue et la complexité du cadre réglementaire français de la sécurité des systèmes d'information et de la confiance numérique, détaillées dans les sections précédentes de ce rapport, soulignent la difficulté potentielle pour les non-spécialistes, voire pour les professionnels, d'accéder rapidement à l'information pertinente et de naviguer au travers des nombreux textes et concepts. Dans une démarche visant à faciliter l'accès et la consultation des informations contenues dans ce rapport, un outil interactif a été développé.

Ce développement a donné naissance à un chatbot conversationnel basé sur l'intelligence artificielle. Sa particularité réside dans le fait qu'il a été spécifiquement entraîné et affiné en utilisant les informations contenues dans ce rapport. Cette formation ciblée lui permet d'avoir une connaissance approfondie du contenu présenté, couvrant les deux grands champs d'application : la sécurité des systèmes d'information et la confiance numérique, ainsi que les principales réglementations, directives et articles de loi détaillés.

Le chatbot utilise le modèle Gemini 2.0, une technologie d'IA développée par Google, connue pour ses capacités d'analyse et de génération de texte avancées. Le choix de ce modèle et son affinage sur les données du rapport visent à permettre au chatbot de comprendre les questions des utilisateurs relatives aux lois et réglementations de cybersécurité en France telles que décrites dans le rapport, et de fournir des réponses précises et pertinentes basées exclusivement sur ce corpus d'information.

L'outil a été implémenté sous la forme d'une application web, accessible via une interface utilisateur développée avec le framework Laravel. Cette architecture permet de proposer une expérience utilisateur conviviale et intuitive, où l'utilisateur peut poser ses questions en langage naturel. Le traitement de la question et la génération de la réponse sont effectués en arrière-plan en faisant appel à l'API de Gemini, qui réalise les calculs et l'inférence sur le cloud.

La principale fonction de ce chatbot est d'agir comme un assistant intelligent pour l'exploration du contenu du rapport. Un utilisateur peut, par exemple, poser une question telle que :

"Quelles sont les obligations des OIV selon la LPM 2014-2019 ?"

"Quel est l'objectif du règlement eIDAS ?"

"Comment l'IMI 901 définit-elle la protection des informations sensibles ?"

"Quels sont les dispositifs techniques listés par l'arrêté du 4 juillet 2012 ?"

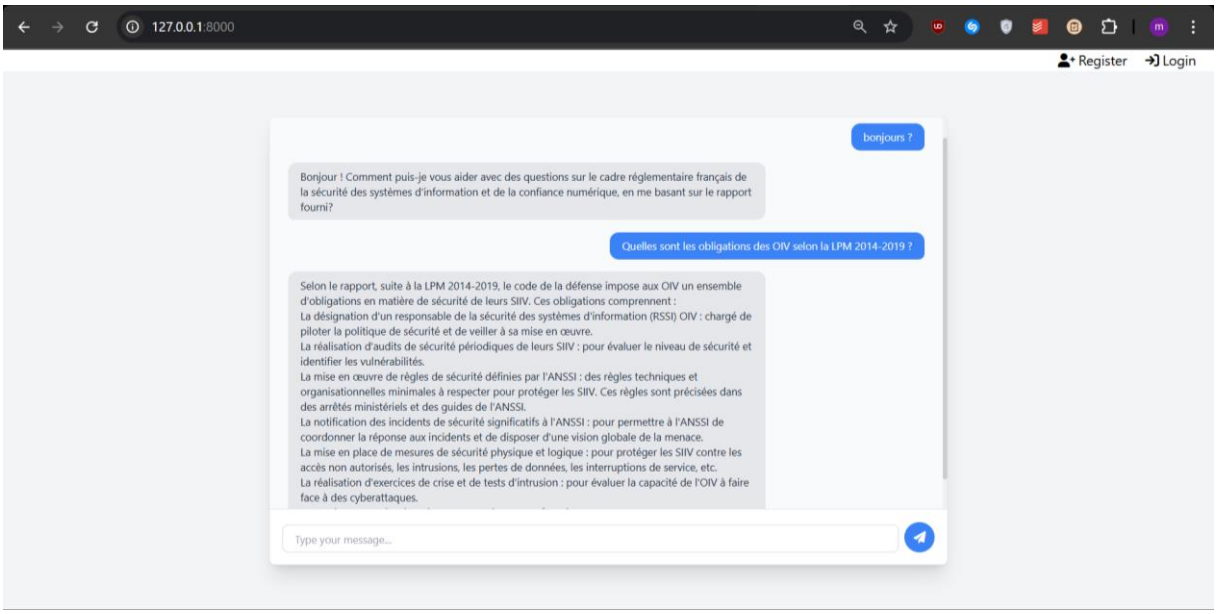

FIGURE 1 EXEMPLE D'UNE CONVERSATION AVEC LE CHATBOT

Le chatbot analysera la question, recherchera les informations pertinentes dans le rapport sur lequel il a été entraîné, et formulera une réponse synthétique basée sur les éléments trouvés. Il peut ainsi aider à clarifier des points spécifiques, à retrouver rapidement une information précise, ou à faire le lien entre différents aspects du cadre réglementaire selon la perspective et les détails offerts par ce document.

Il est crucial de noter que, bien que formé sur un rapport décrivant un cadre juridique, ce chatbot est un outil d'accès à l'information basée sur un document spécifique et ne constitue en aucun cas un conseil juridique formel. Ses réponses se limitent aux informations fournies dans ce rapport et ne prennent pas en compte les évolutions réglementaires postérieures à la rédaction du rapport, les interprétations de la jurisprudence, ou les cas d'application spécifiques qui nécessiteraient l'expertise d'un professionnel du droit. Il s'agit d'une interface intelligente pour interroger un corpus de texte structuré, rendant l'information plus accessible et interactive.

En somme, ce chatbot IA représente une application concrète de l'intelligence artificielle au service de la diffusion et de la consultation de l'information réglementaire complexe. En capitalisant sur le contenu exhaustif de ce rapport, il offre aux utilisateurs un moyen rapide et interactif d'appréhender les principaux aspects du cadre réglementaire français de la cybersécurité et de la confiance numérique, tel que présenté dans ce document.

Lien du projet en GitHub : https://github.com/someone2042/example-app

Conclusion Générale

À l'issue de cette analyse, portant sur le cadre réglementaire français de la sécurité des systèmes d'information et de la confiance numérique, plusieurs conclusions majeures peuvent être retenues. La France s'est d'abord doter d'un dispositif ambitieux, organisé autour de deux piliers : la sécurité des systèmes d'information, d'une part, et la confiance numérique, d'autre part. Si ces deux piliers sont bien distincts, ils sont complémentaires et visent à bâtir un environnement numérique sûr, fiable et favorable au développement économique et social.

Le cadre réglementaire de la sécurité des systèmes d'information repose sur une démarche précautionneuse, mais également sectorielle. Il prend en considération la multiplicité des enjeux et des risques associés à la numérisation de la société et détermine les exigences réglementaires en tenant compte de ces enjeux et de ces risques, passant de la protection du secret de la défense nationale au traitement des infrastructures critiques et des services essentiels, en passant par la sécurisation des informations sensibles et des systèmes d'information de l'État, ce qui témoigne de la richesse et de l'adaptabilité du dispositif législatif. L'effort est particulier sur la prévention, la détection, la réponse aux incidents et la responsabilisation des acteurs, publics comme privés.

Le cadre juridique de la confiance numérique constitue un levier pour enrichir la cybersécurité d'une approche plurielle mobilisant la fiabilité, la transparence, le respect des droits fondamentaux. Il cherche à établir un cadre d'interactions et d'échanges en cyberespace sécurisés entre les citoyens et les entreprises. Il repose sur la sécurité des échanges, la certification de la cybersécurité, le contrôle de la cryptographie et de la vie privée. Mais ces volets se situent au cœur d'un cadre européen désormais harmonisé, autour de règlements phares comme l'eIDAS et le Cybersecurity Act, tout en gardant des spécificités nationales adaptées à la France.

L'élément le plus central du cadre réglementaire étudié est bien évidemment l'institution que représente l'ANSSI. L'ANSSI est bien l'autorité pivot, responsable de la définition et de la diffusion des règles de sécurité, ainsi que de leur contrôle, de l'accompagnement à la mise en œuvre par les acteurs, de la détection et de la réponse aux incidents tout en garantissant un bon niveau de cybersécurité au sein du pays. Son expertise technique d'une part et son indépendance d'autre part lui donnent un rôle central dans les dispositifs de cybersécurité et de confiance numérique en France.

Cette analyse du cadre réglementaire exhibe une recherche constante de compromis, entre le besoin de renforcer la sécurité et la confiance dans le numérique et la nécessité de ne pas brider les dispositifs d'innovation et de développement économique, entre les exigences de sécurité et de respect des libertés individuelles, à commencer par le droit au respect de la vie privée et du secret des correspondances. Cet équilibre se matérialise dans des réglementations souvent précises et nuancées, cherchant motifs à concilier des objectifs parfois antagonistes.

Enfin, il est important de souligner le caractère dynamique et évolutif du cadre réglementaire français. Face à l'évolution rapide des technologies et des menaces cybernétiques, la France adapte régulièrement ses réglementations, en intégrant les nouvelles directives européennes

(comme NIS 2), en actualisant les référentiels normatifs (comme le RGS), et en renforçant les dispositifs de contrôle et de sanction. Cette capacité d'adaptation est essentielle pour maintenir l'efficacité du cadre réglementaire et garantir un niveau de cybersécurité et de confiance numérique élevé dans la durée.

En conclusion, le cadre réglementaire français de la sécurité des systèmes d'information et de la confiance numérique témoigne d'une ambition forte de la France de se positionner comme un acteur majeur de la cybersécurité et de la confiance numérique en Europe et dans le monde. Il constitue un atout important pour garantir la sécurité de l'économie numérique, protéger les citoyens et les entreprises contre les cybermenaces, et favoriser le développement d'un cyberespace de confiance, indispensable à la prospérité et à la souveraineté numérique de la France.

Reference

Note Importante : La structure et les titres de toutes les parties de ce rapport sont basés sur l'article "S'informer sur la réglementation" publié sur le site officiel cyber.gouv.fr**.** Ceci a été fait afin de refléter l'organisation officielle de l'information sur le cadre réglementaire français de la sécurité du numérique et de faciliter la consultation et la vérification des informations.

Mots clés et acronymes

Instruction Générale Interministérielle 1300 (IGI 1300)

Instruction Interministérielle 910 (IMI 910)

Instruction Interministérielle 300 (IMI 300)

Instruction Interministérielle 2100 (IMI 2100)

Instruction Générale Interministérielle 2102 (IGI 2102)

Décret n° 2011-245 du 3 mars 2011 relatif à la protection du potentiel scientifique et technique de la nation (PPST)

Instruction Interministérielle 901 (IMI 901)

Loi de Programmation Militaire 2014-2019 (LPM 2014-2019)

Directive (UE) 2016/1148 (Directive NIS)

Décret n° 2022-513 du 8 avril 2022 relatif à la gouvernance de la sécurité numérique de l'État

Politique de Sécurité des Systèmes d'Information de l'État (PSSIE)

Article L.33-14 du code des postes et communications électroniques (CPCE)

Référentiel Général de Sécurité (RGS)

Règlement (UE) n° 910/2014 (Règlement eIDAS)

Articles L.100 à L.103 du code des postes et communications électroniques (CPCE)

Règlement (UE) 2019/881 (Cybersecurity Act)

Loi n°2004-575 du 21 juin 2004 (LCEN)

Règlement délégué (UE) 2019/2199

Articles R.226-1 et suivants du code pénal

Arrêté du 4 juillet 2012

- **SSI:** Sécurité des Systèmes d'Information
- **ANSSI:** Agence Nationale de la Sécurité des Systèmes d'Information
- **OIV:** Opérateur d'Importance Vitale
- **OSE:** Opérateur de Services Essentiels
- **FSN:** Fournisseur de Services Numériques
- **EI:** Entité Importante
- **EE:** Entité Essentielle
- **SIIV:** Systèmes d'Information d'Importance Vitale
- **SIE:** Systèmes d'information de l'État
- **PST:** Patrimoine Scientifique et Technique
- **ZRR:** Zones à Régime Restrictif
- **PPST:** Dispositif de Protection du Patrimoine Scientifique et Technique
- **RGS:** Référentiel Général de Sécurité
- **LCEN:** Loi pour la Confiance dans l'Économie Numérique
- **eIDAS:** electronic IDentification, Authentication and trust Services
- **NIS:** Network and Information Security Directive
- **NIS 2:** Directive (UE) 2022/2555
- **CMSN:** Comité Ministériel de la Sécurité Numérique
- **ANCC:** Autorités nationales de certification de cybersécurité
- **ENISA:** Agence de l'Union européenne pour la cybersécurité
- **TEMPEST:** Telecomunications Electronics Material Protected from Emanating Spurious Transmissions

Dans le cadre de cette analyse, l'intelligence artificielle a été utilisée comme outil d'assistance pour décortiquer et synthétiser les lois, dont la complexité et la longueur nécessitaient une approche méthodique. L'IA a permis d'identifier les éléments clés, de clarifier les concepts juridiques et de condenser l'information en un format plus accessible, facilitant ainsi la compréhension des enjeux et des implications de cette législation. L'IA a été aussi utilisée pour améliorer la qualité de l'écriture

Exemple d'une prompt :

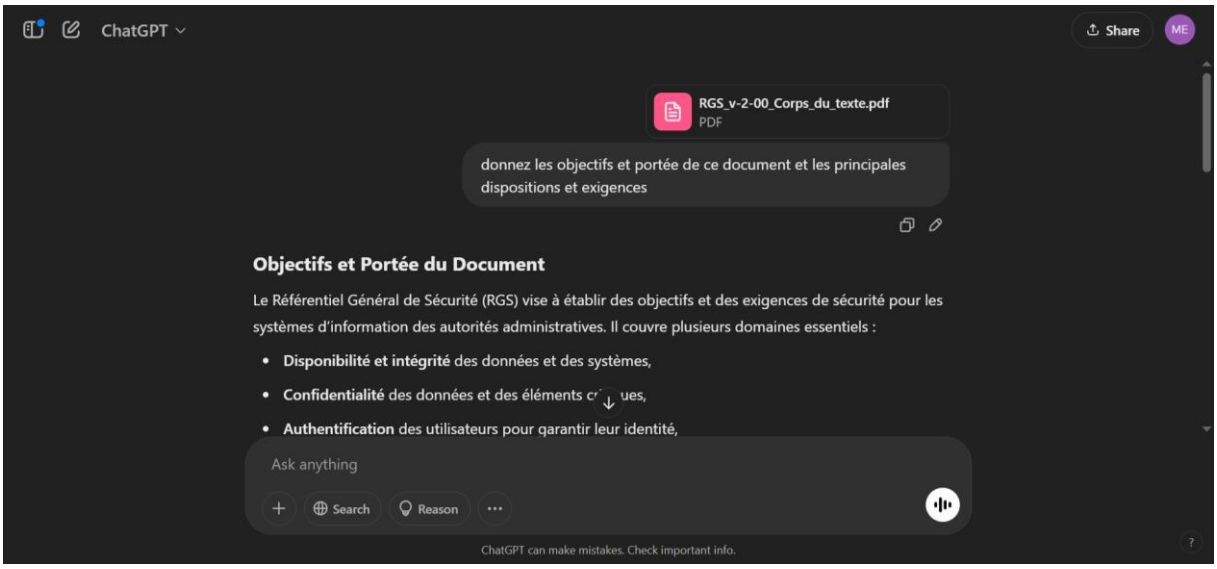

FIGURE 2 EXEMPLE D'UNE PROMPT