الجمهورية الجزائرية الديمقراطية الشعبية
République algérienne démocratique et populaire
وزارة التعليم العالي والبحث العلمي
Ministre de l'enseignement supérieur et de la recherche scientifique

Université Kasdi Merbah Ouargla

Faculté des Nouvelles Technologies
de l'Information et de Communication
Département d'informatique et des
Technologies de l'information

جامعة قاصدي مرباح ورقلة

كلية التكنولوجيات الحديثة للمعلومات والاتصال

قسم الاعلام الالي وتكنولوجيات المعلومات

Mémoire en vue de l'obtention du diplôme de Master
Domaine : Mathématique et Informatique
Filière : Informatique
Spécialité : Informatique fondamentale
THEME :

Application informatique dédiée à la mise en conformité de la loi 18-07 pour la protection des données à caractère personnel

Présenté par : **GUETTAL Redouane**

Les membres du jury :

Président	**Mme. Kaoudja Zineb**	**MCB**	**U.K.M Ouargla**
Examinateur	**Mme. Benkhrourou chafika**	**MAA**	**U.K.M Ouargla**
Encadreur	**M. BENKADDOUR Mohammed Kamel**	**MCA**	**U.K.M Ouargla**

Année universitaire 2023/2024

Remerciements

Tout d’abord, nous tenons à exprimer nos remerciements au « **Bon Dieu** ».

« **Le Généreux qui a enseigné à l'homme ce qu'il ne savait pas** »

De nous avoir donné la volonté, la patience, la force, la foi et le courage pour réaliser ce travail. Merci Allah de nous avoir appris, guidées tout au long de notre vie.

Je remercie l'Université d'Ouargla et le corps professoral du département d'informatique pour m'avoir offert l'opportunité de suivre ce master et d'acquérir des connaissances approfondies dans le domaine de l'informatique. Je suis particulièrement reconnaissant à mon encadreur pour sa direction éclairée, ses conseils précieux et son soutien constant tout au long de mon parcours.

Je suis profondément reconnaissant à ma famille pour leur amour, leur soutien et leurs encouragements constants. Je remercie particulièrement mes chers parents qui m'ont inculqué les valeurs de travail, de persévérance et de rigueur. Je remercie également ma conjointe et mes enfants pour leur compréhension et leur patience pendant que je consacrais mon temps à ce mémoire.

Je remercie également les membres du jury pour nous avoir fait le grand honneur d'examiner et d’évaluer ce travail.

Un grand merci à mes collègues de travail à l’ENTP. Leur compréhension et leur flexibilité m'ont permis de concilier mes responsabilités professionnelles et académiques. Leur soutien moral et leur encouragement ont été essentiels pour surmonter les moments difficiles.

Enfin, je remercie tous ceux qui, de près ou de loin, ont contribué à la réalisation de cette thèse. Vos encouragements et votre soutien ont été d'une grande importance pour moi.

Dédicace

Ce mémoire est dédié à ceux qui m'ont soutenu et inspiré tout au long de ce parcours :

À mes parents,

À ma conjointe,

À mes frères et sœurs

À mes collègues de l'ENTP,

À mes professeurs et à mon encadreur de l'université d'Ouargla,

À mes amis,

À tous ceux qui, de près ou de loin, ont contribué à l'accomplissement de ce projet.

Merci à vous tous.

Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations

AIPD	Analyse d'Impact relative à la Protection des Données
ANPDP	Autorité Nationale de Protection des Données à caractère Personnel
BD	Base de données
DAC	Diagramme d'Activité
DCL	Diagramme de Classe
DCP	Données à Caractère Personnel
DCU	Diagramme de Cas d'Utilisation
ENTP	Entreprise Nationale des Travaux aux Puits
ISO	International Standards Organisation
PC	Personne Concernée
RepH	Représentant Habilité
RGPD	Règlement Général sur la Protection des Données
RSSI	Responsables de la Sécurité des Systèmes d'Information
RT	Responsable du Traitement
SGBD	Système de Gestion de Base de Données
ST	Sous-Traitant
UE	Union Européenne
UML	Unified Modeling Language
UP	Unified Process
VFP	Visual FoxPro

Résumé

Avec la propagation croissante des données personnelles dans le monde, de grandes préoccupations émergent concernant la protection de la vie privée des individus et la confiance dans les systèmes informatiques. Ainsi, l'État algérien a promulgué la loi 18-07 le 10 juin 2018 pour protéger les individus en ce qui concerne le traitement de leurs données personnelles et a établi l'Autorité Nationale de Protection des Données à caractère Personnelles (ANPDP) pour veiller à l'application de cette Loi.

Pour relever ce défi, ce mémoire propose la conception et la mise en œuvre d'une application informatique dédiée à la conformité à la loi 18-07 pour la protection des données personnelles. Pour ce faire, nous avons commencé par recueillir toutes les informations relatives à la protection des données personnelles dans le traitement à partir des lois et réglementations actuelles, puis les avons traduites dans la phase de conception en utilisant des diagrammes UML pour obtenir des diagrammes de cas d'utilisation, d'activités et de classes, en utilisant la méthodologie UP.

Pour renforcer la protection des données personnelles et assurer une gestion efficace de ces données, il était nécessaire de mettre en œuvre un système de gestion de base de données et les techniques de la cryptographie, le langage de programmation Microsoft Visual FoxPro V.9 a été utilisé pour développer la base des données et les différentes interfaces et états de sorties du système.

L'application a été testée en mettant en œuvre une étude de cas réelle au sein de l'Entreprise Nationale des Travaux aux Puits (ENTP). Cette étude de cas est composée d'un traitement de données personnelles, d'un droit de la personne concernée et d'une violation des données personnelles.

Mots clefs : Loi 18-07- Autorité Nationale de Protection des Données à caractère Personnel - Protection des données à caractère personnel - Diagrammes d'UML - Cryptographie – Traitement des données personnelles - Droits des personnes concernées – Violation des données personnelles.

Abstract

With the increasing spread of personal data worldwide, significant concerns have emerged regarding individuals' privacy protection and trust in computer systems. As a result, the Algerian state promulgated Law 18-07 on June 10, 2018, to protect individuals concerning the processing of their personal data and established the National Authority for the Protection of Personal Data (ANPDP) to ensure the application of this law.

To address this challenge, this thesis proposes the design and implementation of a software application dedicated to compliance with Law 18-07 for the protection of personal data. To achieve this, we began by gathering all relevant information on personal data protection in processing from current laws and regulations, then translated these into the design phase using UML diagrams to create use case, activity, and class diagrams, employing the UP methodology.

To enhance personal data protection and ensure efficient management of this data, it was necessary to implement a database management system and cryptography techniques. Microsoft Visual FoxPro V.9 was used to develop the database and the various system interfaces and output reports.

The application was tested by implementing a real case study within the National Company for ENTP. This case study comprised personal data processing, the right of the concerned person, and a personal data breach

Keywords: Act 18-07- National Authority for the Protection of Personal Data - Personal Data Protection - UML diagrams – Cryptography - Personal Data Processing - Rights of Data Subjects - Personal Data Breach.

ملخص

مع انتشار البيانات الشخصية بشكل متزايد في العالم، تثار مخاوف كبيرة بشأن حماية خصوصية الفرد والثقة في النظم المعلوماتية، أصدرت الدولة الجزائرية قانون 18-07 في 10 جوان 2018 لحماية الأفراد فيما يتعلق بمعالجة بياناتهم الشخصية وقد أنشأت السلطة الوطنية لحماية المعطيات ذات الطابع الشخصية لضمان تطبيق هذا القانون.

للتغلب على هذا التحدي، تقترح هذه المذكرة تصميم وتنفيذ تطبيق معلوماتي مخصص للامتثال لقانون 18-07 لحماية البيانات الشخصية ولتحقيق ذلك، بدأنا بجمع جميع المعطيات المتعلقة بحماية البيانات الشخصية في المعالجة وترجمتها في مرحلة التصميم إلى مخططات UML للحصول على مخطط حالات الاستخدام (DCU)ومخططات الأنشطة (DAC) ومخططات الصفوف (DCL) مستعينين بمنهجية UP.

من أجل تعزيز حماية البيانات الشخصية والتسيير الفعال لهذه المعطيات، كان من الضروري تنفيذ نظام إدارة قواعد البيانات وتقنيات التشفير، تم استخدام مايكروسوفت فيجوال فوكس برو كلغة برمجة لتطوير قاعدة البيانات والواجهات المختلفة والتقارير الناتجة عن التطبيق.

تم اختبار التطبيق من خلال تنفيذ دراسة حالة حقيقية داخل المؤسسة الوطنية لأشغال في الآبار. تتكون هذا الدراسة من معالجة البيانات الشخصية، وحق الشخص المعني بالبيانات، وقضايا انتهاك البيانات.

مصطلحات: قانون 18-07، السلطة الوطنية لحماية المعطيات ذات الطابع الشخصية، حماية البيانات الشخصية، مخططاتUML ، التشفير، معالجة المعطيات الشخصية، حقوق الأشخاص المعنيين، انتهاك البيانات الشخصية.

Introduction générale

Dans un monde de plus en plus digitalisé, la gestion et la protection des données personnelles sont devenues des enjeux cruciaux pour les entreprises et les gouvernements. La rapidité de la circulation des informations et l'omniprésence des technologies posent des défis considérables en matière de sécurité et de confidentialité des données.

L'omniprésence des données personnelles et leur circulation rapide à travers les frontières dans un monde où la technologie a gagné tous les domaines, soulèvent des préoccupations majeures quant à la préservation de la vie privée individuelle et à la confiance dans les systèmes informatiques. La conformité aux lois de protection des données devient ainsi une nécessité impérieuse pour garantir l'assurance et la sécurité dans les environnements technologiques, où les données personnelles sont collectées, stockées et partagées à un rythme sans précédent.

En Algérie, l'adoption de la loi 18-07 en 2018 représente une avancée significative dans la protection des données à caractère personnel. Cette loi, inspirée des normes internationales, vise à encadrer la collecte, le traitement et l'utilisation des données personnelles par les organisations. Elle joue un rôle crucial dans le renforcement de la confiance entre les consommateurs et les prestataires de services, ce qui est essentiel pour stimuler les économies numériques. Toutefois, le respect de cette loi pose des défis techniques et organisationnels auxquels les entreprises doivent faire face.

C'est dans cette même optique que s'inscrit le thème de la présente étude portant sur ''le développement d'une application informatique dédié à la mise en conformité de la loi 18-07 pour la protection des données à caractère personnel '', ce choix motivé par le contexte décrit ci-haut, a pour but de contribuer modestement aux efforts déployés par les organisations pour se doter des outils de protection des données et aussi aménager un meilleur équilibre entre d'une part, l'utilisation des technologies nouvelles et d'autre part, la protection de la vie privée des personnes contre les risques de violations engendrés par l'évolution rapide de ces mêmes technologies.

La solution préconisée par notre étude se voit être un outil d'appui mis à disposition des entreprises pour la mise en conformité des traitements des données à caractère personnel par rapport aux dispositions et spécificités énoncées dans la loi 18-07, offrant une interface conviviale, des évaluations de conformité automatisées et des conseils personnalisés ; de tels produits sont rares actuellement sur le marché local, vu que le besoin de protection des données à caractère personnel n'était pas une priorité majeure au sein de nos entreprises par manque de loi les obligeant à se conformer.

Problématique

La problématique à laquelle nous espérons que ce modeste travail va donner solution réside dans les défis et contraintes que rencontrent les entreprises et organisations opérant en Algérie dans l'application de la nouvelle loi 18-07 relative à la protection des personnes physiques dans le traitement des données à caractère personnel ; ces difficultés peuvent être résumées à travers les aspects suivants :

1. Compréhension des exigences légales : Les organisations font face à des obstacles dans la compréhension des exigences précises imposées par la Loi 18-07, ce qui complique leur capacité à se conformer efficacement.

2. Mise en place des mesures techniques et organisationnelles : La mise en place de mesures adéquates pour protéger les données personnelles nécessite des efforts considérables, tant sur le plan technique qu'organisationnel.

3. Implémentation des droits des personnes concernées : Les entreprises éprouvent des difficultés à mettre en œuvre les droits des individus, tels que le droit d'accès, de rectification et d'opposition aux traitements de leurs données personnelles.

4. Identification des lacunes dans les systèmes informatiques : Il est crucial pour les organisations de détecter et de combler les lacunes dans leurs systèmes informatiques, notamment celles relatives à la gestion et à la sécurisation des données personnelles.

5. Risques potentiels liés à la non-conformité : Les entreprises qui ne respectent pas la loi 18-07 s'exposent à divers risques, notamment des sanctions légales et des préjudices impactant leur réputation.

Les solutions disponibles pour aider les organisations à se conformer à la loi 18-07 sont limitées. D'une part, sur le marché algérien, aucune solution n'est disponible en raison du caractère récent de l'entrée en vigueur de la loi. D'autre part, les outils existants sur le marché international peuvent être coûteux, complexes à utiliser et ne prennent pas toujours en compte les particularités de la législation algérienne.

Objectif de l'étude

L'objectif de la réalisation de la présente étude pour l'obtention d'un master en informatique de l'Université d'Ouargla consiste à l'accomplissement des deux volets suivants :

1. **Développement d'une application informatique dédiée à la mise en conformité de la loi 18-07 pour la protection des données à caractère personnel** :
   - Développer une application dédiée pour aider les organismes et les entreprises, qu'ils soient publics ou privés, à se conformer à la loi 18-07 en Algérie.
     Une étude de cas sera menée au sein de l'Entreprise Nationale des Travaux aux Puits (E.N.T.P.), filiale de la Sonatrach spécialisée dans le forage pétrolier, située à Hassi-Messaoud (Ouargla) employés et disposant d'un système d'information ERP.
   - L'application s'articule sur les trois modules suivants :
     a. *Gestion des traitements des données à caractère personnel* : suivre les différentes opérations de traitement des données personnelles.
     b. *Gestion des droits des personnes concernées* : permettre aux individus d'exercer leurs droits d'accès, de rectification et d'opposition au traitement de leurs données personnelles, tels que garantis par la loi.
     c. *Gestion des violations de données à caractère personnel* : identifier, documenter et répondre efficacement aux incidents de sécurité impliquant des données personnelles.

2. **Proposition de solutions techniques et organisationnelles** :
   - L'application une fois mise en œuvre mettra à disposition de l'organisation utilisatrice les mesures techniques et organisationnelles nécessaires pour prévenir la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé aux données à caractère personnel. Ces mesures sont particulièrement requises lors des transferts de données via des réseaux.
   - L'utilisation assidue de l'application garantira l'implémentation des mesures prévues dans chaque article de la loi 18-07 dans la gestion courante des organisations, assurant ainsi leur parfaite conformité avec la loi.

En effet, ces deux volets combinent le développement pratique d'un outil de conformité avec des recommandations stratégiques pour sécuriser et améliorer la gestion des données personnelles, assurant ainsi une approche holistique et efficace de la protection des données en Algérie.

Organisation du mémoire

Ce mémoire est structuré en quatre chapitres principaux :

Le premier chapitre explore les concepts fondamentaux ainsi que l'importance de la protection des données personnelles.

Le deuxième chapitre présente l'Autorité nationale de protection des données à caractère personnel et détaille les dispositions de la loi 18-07.

Le troisième chapitre se consacre à la conception d'un outil informatique visant à protéger les données personnelles et à proposer des solutions techniques et organisationnelles pour se conformer à la loi 18-07.

Le quatrième chapitre se focalise sur l'implémentation pratique et la réalisation de l'application développée dans le cadre de cette thèse.

Enfin, le mémoire se termine par une conclusion générale comportant un aperçu sur les résultats obtenus et des commentaires et des propositions de perspectives futures pour des travaux complémentaires de recherche et développement dans ce domaine.

Chapitre 1

La protection des données à caractère personnel

1 Introduction

Avec l'avancement de la technologie et l'utilisation généralisée d'Internet, les individus produisent et diffusent d'importantes quantités d'informations personnelles en ligne, transcendant les frontières nationales. Cette collecte de données vise à faciliter l'échange et l'exploitation de ces informations dans divers secteurs commerciaux, politiques et économiques, souvent au détriment des normes de protection de la vie privée et de la dignité individuelle.

Ces enjeux soulèvent des préoccupations majeures quant à la confidentialité et à la sécurité des données, étant donné le potentiel d'exploitation des informations personnelles à des fins telles que le vol d'identité, la fraude et l'accès non autorisé à des données sensibles. En réponse à ces défis, de nombreux pays ont instauré des dispositifs législatifs, réglementaires et technologiques visant à garantir la protection des données à caractère personnel.

2 Définitions

Ce paragraphe porte sur la définition des concepts les plus pertinents en relation avec la protection des DCP.

2.1 La vie privée

La vie privée est « le droit d'un individu de déterminer quand, comment et dans quelle mesure ces informations sont communiquées à d'autres », comme définie par Alain F. Westin **[1]**.

D'après Sara Basse **[2]**, la vie privée signifie globalement : l'absence d'intrusion, le contrôle des informations nous concernant et l'absence de surveillance.

2.2 Les données à caractère personnel

D'après Ibrahim Coulibaly **[3]**, le concept DCP est fondé sur quatre éléments principaux, à savoir : « toute information », « concernant », « personne physique », « identifiée ou identifiable ».

Selon la CNIL **[4]**, c'est toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement ; par exemple : un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, etc.

2.3 Les données sensibles

Les experts **[5]** définissent la donnée sensible comme étant les informations qui doivent être protégées contre l'accès non autorisé ou la divulgation ; elles peuvent inclure :

- Renseignements personnels
- Renseignements personnels sur la santé
- Dossiers scolaires
- Dossiers clients
- Informations financières
- Renseignements d'ordre criminel
- Renseignements géographiques
- Renseignements personnels confidentiels
- Renseignements jugés confidentiels ; données confiées à une tierce personne, à une organisation ou à une entité dans l'intention d'en préserver la confidentialité en interdisant ou en limitant les droits d'accès.
- Renseignements protégés en vertu de toute politique interdisant l'accès non autorisé.

2.4 Traitement des données à caractère personnel

Est considéré comme traitement des DCP, toute manipulation de données personnelles, quels que soient les moyens utilisés **[4]**, cela englobe diverses actions telles que la collecte, l'enregistrement, l'organisation, la conservation, la modification, l'association avec d'autres données, la transmission, etc.

Ces traitements ne se limitent pas aux fichiers, bases de données ou tableaux Excel, mais incluent également des dispositifs tels que la vidéosurveillance, les systèmes de paiement par carte bancaire, la reconnaissance biométrique, les applications pour smartphone, etc. Ils évoluent en fonction des avancées technologiques et peuvent être informatisés ou manuels, comme des dossiers papier classés par ordre alphabétique ou chronologique.

3 Cadre juridique

Dans de nombreuses juridictions, sur le plan international ou local, des lois et règlements spécifiques ont été légiférés pour protéger les DCP.

Ces cadres juridiques décrivent les droits des individus à l'égard de leurs renseignements personnels et établissent des obligations pour les organisations qui collectent et traitent les données**.**

3.1 Sur le plan international

Adopté en 2016 et entré en vigueur en 2018, le Règlement général sur la protection des données (RGPD) établit un ensemble de règles pour le traitement des données à caractère personnel des citoyens de l'UE plus les quatre États de l'Association Européenne de Libre Echange ‘’l'AELE’’ (Liechtenstein, Norvège, Islande et Suisse**) [5]**.

Vient après l'ISO avec sa norme ISO/IEC 27701 publiée en août 2019, et qui a défini pour la première fois les exigences pour les systèmes de management de protection de la vie privée **[6]**.

Enfin, l'Afrique est le continent le moins doté en matière de législation spécifique à la protection des données à caractère personnel, où seulement 36 pays parmi les 55 qui forment le continent, possèdent des lois entièrement dédiées à ce domaine **[7]**.

3.2 Sur le plan local

La protection de la vie privée est consacrée dans la Constitution algérienne depuis 2020 à travers l'article 47 qui stipule : « Toute personne a droit à la protection de sa vie privée et de son honneur…La protection des personnes dans le traitement des données à caractère personnel est un droit fondamental, la loi punit toute violation des droits susmentionnés » **[8]**.

Avant cet engagement, des lois et décrets relatifs à la protection des données ont été établis pour faire face à l'évolution rapide de l'utilisation de l'Internet et des nouvelles technologies de communication, à savoir :

- Le décret exécutif n° 98-257 du 25 aout 1998 définissant les conditions et modalités de mise en place et d'exploitation des services Internet, son article 14 précise : « …garder confidentielle toute information relative à la vie privée de ces abonnés… » **[37]**

- La loi 09-04 du 05/08/2009 portant sur la définition des règles particulières de prévention et de lutte contre les infractions liées aux technologies de l'information et de la communication **[9]**

- La loi 18-04 du 10/05/2018 fixant les règles générales relatives à la poste et aux communications électroniques **[10]**

- La loi 18-07 du 10/06/2018 portant sur la protection des personnes physiques dans le traitement des données à caractère personnel, cette loi est effective à partir du 10/08/2023 **[11]**

- Le décret présidentiel 20-05 du 20/01/2020 visant à instaurer un dispositif national de la sécurité des systèmes d'information **[12]**.

4 Protection des données personnelles et les systèmes d'information

Les analyses des textes légaux et réglementaires ainsi que des chartes d'utilisation des systèmes informatiques ont fait ressortir les six axes sur lesquels la protection des données personnelles s'articule **[14]**, à savoir :

1. **Information** : l'obligation d'informer l'utilisateur sur les traitements,
2. **Consentement** : l'accord exprimé par le propriétaire des données, à la collecte et au traitement de ses informations personnelles,
3. **Modification** : regroupe plusieurs droits du propriétaire des données, entre autres : l'accès, la mise à jour et la suppression des données collectées et traitées,
4. **Justification** : justifier la finalité du traitement des données en répondant à la question : « *Est-il justifié de collecter telle donnée et de l'utiliser dans le cadre de tel traitement ?* »
5. **Conservation** : la durée de conservation des données personnelles est limitée dans le temps et déterminée selon le contexte du traitement,
6. **Transmission** : la transmission des données à des tiers doit être limitée et soumise à autorisation, dans certains cas spéciaux, elle est carrément interdite.

Dans les systèmes d'information, ces axes se traduisent sous la forme de lignes directrices, telles que **la protection des données dès la conception**, **l'évaluation de l'impact sur la vie privée** et **la notification des violations de données [15]**.

Ces lignes directrices vont être développées séparément dans les paragraphes suivants.

4.1 Protection de la vie privée dès la conception

La protection des données personnelles doit être prise en charge dès la conception des systèmes, et ceci en intégrant les sept principes suivants **[16]** :

1. Proactif et non réactif, préventif et non correctif
2. Protection des données comme paramètre par défaut
3. Protection des données intégrée dans la conception
4. Fonctionnalité complète
5. Sécurité de bout en bout
6. Visibilité et transparence
7. Respect de la vie privée des utilisateurs

La protection des données dès la conception est un processus impliquant divers composants **technologiques** et **organisationnels**, qui mettent en œuvre des principes de confidentialité et de protection des données **[17]**.

Le chercheur Jaap-Henk Hoepman a défini les huit stratégies ci-dessous citées, que les architectes informaticiens doivent suivre pour la prise en charge de

la protection de la vie privée dès la conception, comme démontré dans la figure 1.1 **[45]** :

1. **Minimiser** : consiste à minimiser les impacts possibles d'un système sur la vie privée, en ne collectant que les données nécessaires pour un traitement.
2. **Cacher** : Les données personnelles et leurs interrelations doivent être cachées à la pleine vue afin d'éviter tout abus les concernant (ex. cryptage des données).
3. **Séparer** : la séparation implique que les données personnelles doivent être traitées de manière distribuée, dans des compartiments séparés dès que possible (ex. : K-anonymity, l-Diversity).
4. **Agréger** : la stratégie « Agréger » exige que les données personnelles soient traitées au plus haut niveau d'agrégation et avec le moins de détails possible.
5. **Informer** : fait référence à la transparence, ce qui exige que les propriétaires des données soient informés de façon adéquate lors du traitement de leurs informations.
6. **Contrôler** : cela consiste à donner à la personne concernée le plein droit et le plein contrôle sur ses données personnelles.
7. **Imposer** : cette stratégie exige qu'une politique de confidentialité compatible avec les exigences légales doive être en place et doit être appliquée.
8. **Démontrer** : le responsable de traitement des données doit être en mesure de démontrer le respect de la politique de confidentialité et de toutes les exigences légales applicables.

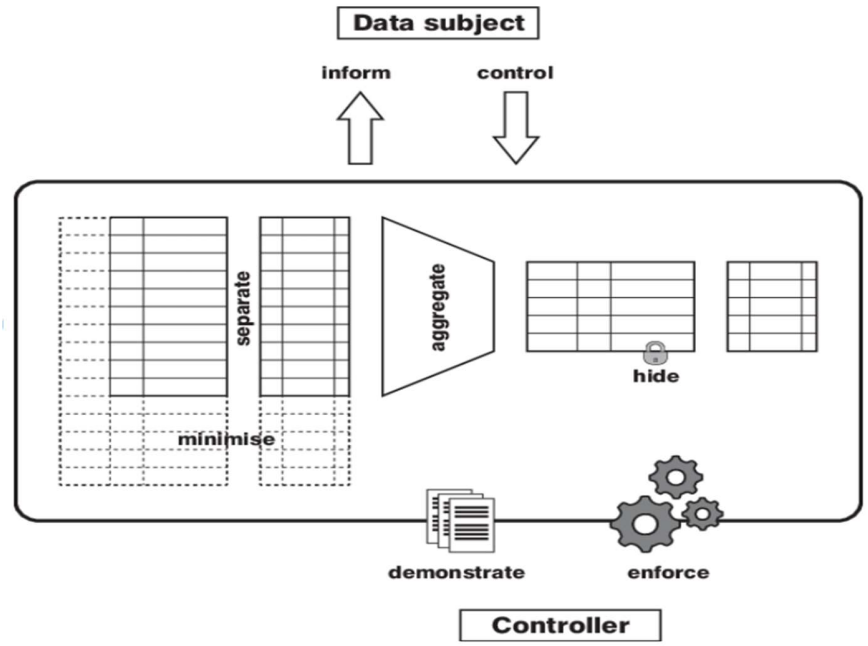


Figure 1.1 : Schéma des huit stratégies de conception de la confidentialité

4.2 Évaluation de l'impact sur la vie privée

Un risque est un scénario qui décrit un événement et ses effets, estimés en termes de gravité et de probabilité. La gestion du risque peut, quant à elle, se définir comme un ensemble d'activités coordonnées dans le but de diriger et de piloter un organisme vis-à-vis du risque **[4]**.

L'analyse d'impact relative à la protection des données (AIPD) est un processus qui permet d'identifier, d'évaluer et de réduire les risques liés à la vie privée **[19]**.

L'objectif principal d'une AIPD est d'analyser le traitement des données à caractère personnel et de déterminer le niveau du risque, comme illustré dans la figure 1.2. Les résultats d'une AIPD permettront à l'organisme de concevoir ses systèmes avec des niveaux de protection des données appropriés.

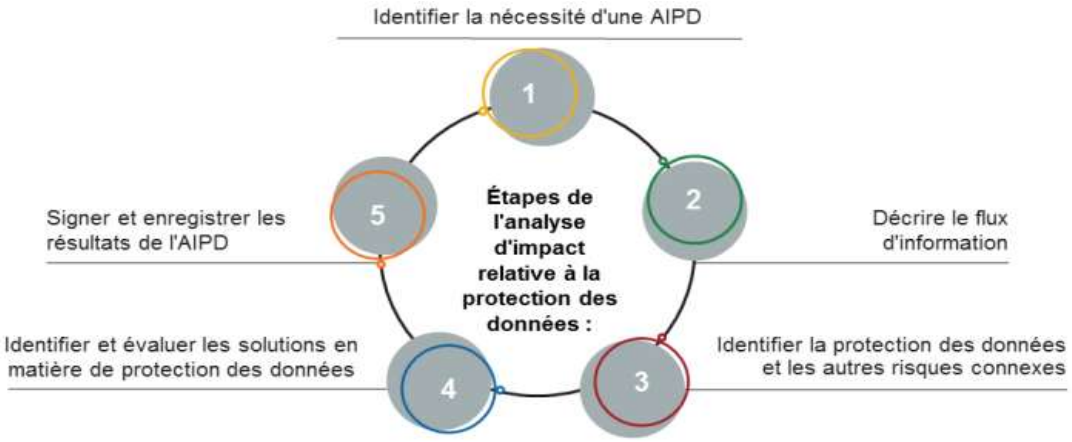


Figure 1.2 : Principales étapes d'une AIPD

Une AIPD est nécessaire quand le traitement est « susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes concernées » **[4]** :

1) Soit le traitement envisagé figure dans la liste des types d'opérations de traitement nécessitant une AIPD propre à la CNIL.
2) Soit le traitement remplit au moins deux des neuf critères suivants :
   - Évaluation/scoring (y compris le profilage) ;
   - décision automatique avec effet légal ou similaire ;
   - Surveillance systématique ;
   - Collecte de données sensibles ou de données à caractère hautement personnel ;
   - Collecte de données personnelles à large échelle ;
   - Croisement de données ;
   - personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
   - Usage innovant (utilisation d'une nouvelle technologie) ;
   - Exclusion du bénéfice d'un droit/contrat.

4.3 Notification des violations des données à caractère personnel

Un incident de sécurité de l'information est un évènement de sécurité de l'information qui a une probabilité significative de menacer les opérations de sécurité de l'information. Si un incident de la sécurité de l'information affecte les DCP, il peut être classé comme une violation des données.

Une violation de DCP est définie comme une atteinte à la sécurité qui entraine la destruction inappropriée ou illégale et la reproduction, la perte ou la modification non autorisée de DCP stockées ou traitées. Cela peut inclure la perte de contrôle sur leurs DCP, la limitation de leurs droits, la discrimination, le vol ou l'usurpation d'identité, la perte financière, le renversement non autorisé du processus de pseudonymisation, l'atteinte à la réputation et la perte de confidentialité de DCP protégées par le secret professionnel **[20]**.

Les types de violations de DCP peuvent être classés en trois catégories :

1) **Violation de la confidentialité** : la divulgation ou l'accès non autorisés ou accidentels à la DCP,
2) **Violation de l'intégrité** : l'altération non autorisée ou accidentelle de DCP,
3) **Violation de la disponibilité** : la destruction ou la perte accidentelle ou non autorisées de l'accès à des DCP.

En cas de violation, un plan d'intervention doit être suivi basé sur les étapes suivantes **[20]** :

1) **Confinement** : cette mesure limite l'impact de la violation de DCP et empêche que ces violations ne se reproduisent ou s'aggravent, ça comprend :
    a. Isolement ou fermeture du système
    b. Désactivation de différentes opérations
    c. Blocage de l'accès aux domaines, serveurs, ports, etc.
    d. Création d'une copie du système
    e. Suspension des pouvoirs avec accès privilégié aux DCP.
2) **Eradication** : étape nécessaire pour trouver des solutions contre les effets de violation des DCP après que l'incident a été contenu.
3) **Récupération** : c'est le fait de rétablir les opérations dans leur état initial et de prévenir la répétition des mêmes violations de DCP.

L'organisme devrait documenter les détails de toutes ces étapes dans un rapport de résolution et notifier les violations présentant un risque pour les droits et les libertés des personnes à l'autorité de contrôle et, dans certains cas, lorsque le risque est élevé, aux personnes concernées **[4]**. Ce rapport de résolution devrait inclure **[20]** :

- La description détaillée de la violation des DCP
- Les mesures en place au moment de la violation des données
- Les enregistrements des mesures d'intervention

- Les mesures de détection utilisées
- La liste des communications effectuées pendant la réponse.

Quelques exemples de violation des DCP sont présentés dans l'annexe A.

5 Conclusion

Dans ce premier chapitre, nous avons essayé de cerner la notion de données à caractère personnel et démontré la nécessité de la protéger, et ceci en commençant par définir les concepts de base, comme la vie privée, la DCP, les données sensibles et le traitement des données à caractère personnel. Par la suite, puis nous avons défini le cadre juridique sur lequel repose la protection des données à caractère personnel. À cet effet, un recueil des textes juridiques a été présenté comportant les lois et les décrets établis à ce jour sur le plan local et international.

Enfin, le dernier paragraphe de ce chapitre traite de la protection des données à caractère personnel dans les systèmes d'information, dans lequel nous avons développé les trois lignes directrices que les systèmes d'information doivent suivre pour assurer la protection et la pérennité des DCP, à savoir : la protection de la vie privée dès la conception, l'évaluation de l'impact sur la vie privée et enfin la notification des violations des données.

Le chapitre deux (2) suivant sera dédié à l'Autorité Nationale de Protection des Données à caractère Personnel (ANPDP), haute institution algérienne, créée en 2022 pour veiller à la conformité des traitements des données à caractère personnel par rapport aux lois et à la réglementation en vigueur.

Chapitre 2

Autorité Nationale de Protection des Données à caractère Personnel

1 Introduction

Durant les travaux d'un colloque international organisé le 19 février 2024 par la Faculté des sciences politiques et des relations internationales de l'université d'Alger 3 sur « La souveraineté numérique de l'État: politiques et expériences comparées ». Le président de l'ANPDP a déclaré que **[11]** :

- La maîtrise de l'État dans son espace numérique est une confirmation de sa souveraineté ;
- La protection des données personnelles est la première pierre angulaire de la souveraineté numérique ;
- L'utilisation massive a conduit à la collecte de quantités massives de données, stockées dans des bases de données créées ici et là dans le but d'échanger des informations et de les exploiter dans divers domaines commerciaux, économiques et politiques sans tenir compte des normes de confidentialité des individus. Cela a nécessité des lois, des mesures réglementaires et techniques pour protéger les droits et la vie privée de ces individus. Pour atteindre cet objectif, il est essentiel de garantir le stockage des données collectées et des données traitées au niveau national, en s'appuyant principalement sur des compétences nationales chargées de protéger le cyberespace de l'État en fournissant les moyens matériels et logistiques nécessaires pour assurer l'indépendance et le contrôle de la numérisation, renforçant ainsi la souveraineté de l'État ;
- Le texte de loi 18-07, daté du 10 juin 2018, est venu comme un instrument constitutionnel pour établir le cadre juridique spécifique du système de traitement des données dans notre pays et pour faire face aux effets découlant de l'évolution rapide des technologies de l'information et de la communication sur la vie privée, la liberté des individus, leur honneur et leur réputation.

Ces déclarations résument d'une manière non exhaustive les missions de l'ANPDP et les raisons de sa création.

2 Présentation de l'ANPDP

L'Autorité Nationale de Protection des Données à caractère Personnel (ANPDP) est une institution administrative indépendante rattachée fonctionnellement à la Présidence de la République, créée par la loi 18-07 du 10 juin 2018 [22] relative à la protection des personnes physiques dans le traitement des DCP. Le siège de l'ANPDP est situé à Alger (commune de Hydra) **[11]**.

L'ANPDP est chargée de veiller à ce que le traitement des DCP soit mis en œuvre conformément aux dispositions de la présente loi et de s'assurer que l'utilisation des technologies de l'information et de la communication ne comporte pas de menaces au regard des droits des personnes, des libertés publiques et de la vie privée **[22]**.

L'ANPDP a passé plusieurs étapes historiques depuis la promulgation de la loi 18-07 le 10 juin 2018 jusqu'à l'installation de son nouveau président le 16 octobre 2023, comme illustré dans le graphe 2.1.

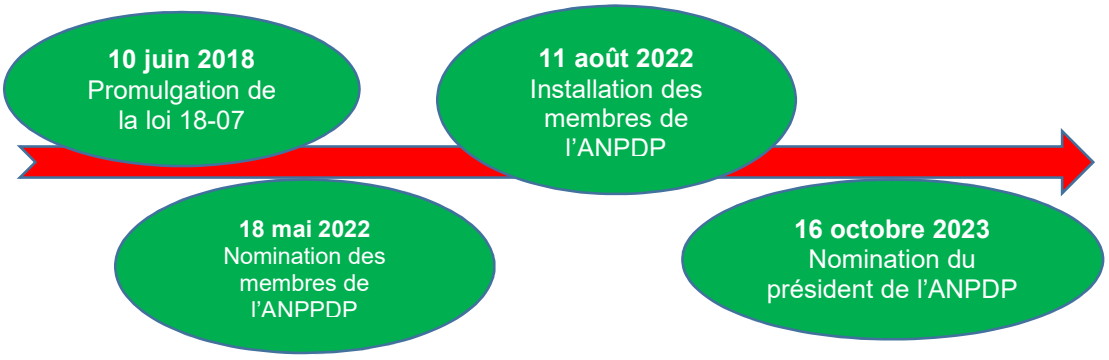


Figure 2.1 : Chronologie de l'ANPDP

3 Organisation de l'ANPDP

L'organisation de l'ANPDP est composée d'un Président, d'un directeur général (secrétariat exécutif) et des membres. Dans l'exécution de ses missions, le directeur général est assisté par deux directeurs d'études et deux chefs d'études. L'organigramme détaillé de l'ANPDP est illustré dans le graphe 2.2 **[22]**:

Figure 2.2 : Organigramme de l'ANPDP

4 Missions de l'ANPDP

L'ANPDP a pour missions **[22]** :

1. De délivrer les autorisations et de recevoir les déclarations relatives au traitement des DCP ;
2. D'informer les PC et les RT de leurs droits et obligations ;
3. De conseiller les personnes et entités qui ont recours aux traitements des données à caractère personnel ou qui procèdent à des essais ou expériences de nature à aboutir à de tels traitements ;
4. De recevoir les réclamations, les recours et les plaintes relatifs à la mise en œuvre des traitements des DCP et d'informer leurs auteurs des suites qui leur sont réservées ;
5. D'autoriser, dans les conditions prévues par la présente loi, les transferts transfrontaliers des DCP ;
6. D'ordonner les modifications nécessaires à la protection des DCP traitées ;
7. D'ordonner la fermeture de données, leur retrait ou destruction ;
8. De présenter toute suggestion susceptible de simplifier et d'améliorer le cadre législatif et réglementaire relatif au traitement des DCP ;
9. De publier les autorisations accordées et les avis émis dans le registre national cité à l'article 28 de la loi 18-07 ;
10. De développer des relations de coopération avec les autorités étrangères similaires, sous réserve de réciprocité ;
11. De prononcer des sanctions administratives dans les conditions définies par l'article 46 de la présente loi 18-07 ;
12. D'élaborer des normes dans le domaine de la protection des DCP ;
13. D'élaborer des règles de bonne conduite et de déontologie applicables aux traitements des DCP.

5 La loi 18-07

La loi n° 18-07 du 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel, constitue une avancée importante en matière de protection des libertés individuelles, mais aussi dans la responsabilisation des entreprises sur les données qu'elles collectent et la préservation de la vie privée des personnes physiques qui interagissent tant dans le processus de production que dans celui de la consommation **[38]**.

La loi 18-07 est structurée en sept titres, comme illustrée dans le tableau 2.1 suivant.

Titres	Chapitres	Articles
1. Dispositions générales		1- 6
1. Principes fondamentaux de protection des DCP	De l'accord préalable et de la qualité des données	7-11
	Des procédures préalables au traitement	12- 21

2. De l'Autorité nationale de protection des données à caractère personnel		22- 31
3. Droits de la PC	Du droit de l'information	32-33
	Du droit d'accès	34
	Du droit de rectification	35
	Du droit d'opposition	36
	Interdiction à la prospection directe	37
4. Des obligations du RT	De la confidentialité et de la sécurité du traitement	38- 41
	Du traitement de DCP liée à la certification et à la signature électronique	42
	Traitement des DCP dans le cadre de communication électronique	43
	Transfert de données vers un pays étranger	44-45
5. Des dispositions administratives et pénales	Des procédures administratives	46-48
	Des règles de procédures	49-53
	Des dispositions pénales	54-74
6. Dispositions transitoires et finales		75-76

Tableau 2.1 : Structure de la loi 18-07

5.1 Principes fondamentaux de protection des données à caractère personnel dans la Loi 18-07

5.1.1 Les données

Les DCP doivent **[22]** :

- Etre traitées de manière licite et loyale,
- Avoir une finalité limitée,
- Etre minimisées,
- Etre exacte,
- Avoir une conservation limitée.

5.1.2 Le Responsable du traitement (RT)

Le RT est tenu de mettre en place des **[22]** :

- Mesures de sécurité techniques et organisationnelles adéquates pour assurer la confidentialité, l'intégrité et la disponibilité des DCP.
- Mécanismes pour que le ST agit uniquement sur instruction de ce dernier.

5.2 Bases juridiques du traitement

Il existe sept bases juridiques auxquelles le traitement doit se conformer **[22]** :

- Le consentement,
- Le contrat avec la PC,
- Les obligations légales,
- La sauvegarde de la vie privée,
- Les intérêts de la PC,
- L'intérêt public,
- Les intérêts légitimes du RT.

5.3 Procédures préalables aux traitements

Le traitement des DCP est soumis **[22]** :

- Soit par une déclaration préalable du traitement à l'ANPDP,
- Soit par l'autorisation préalable de l'ANPDP.

5.3.1 La déclaration du traitement

La déclaration préalable doit contenir les informations suivantes **[22]** :

- Le nom et l'adresse du RT et de RepH,
- La nature, les caractéristiques et la ou les finalités du traitement des données,
- Une description de la catégorie des PC et des DCP,
- Les destinataires ou catégories de destinataires auxquels les données peuvent être divulguées,
- Les transferts envisagés de DCP vers des pays étrangers,
- La durée de conservation des DCP,
- Le service par lequel la PC peut exercer ses droits,
- Une présentation globale permettant d'évaluer initialement l'adéquation des mesures prises pour garantir la confidentialité et la sécurité du traitement,
- Les interconnexions.

5.3.2 L'autorisation du traitement

La demande d'autorisation doit contenir les mêmes informations que dans la demande de déclaration. Elle est destinée pour les trois cas spécifiques suivants **[22]** :

- Données sensibles,
- Interconnexion entre bases de données,
- Transfert de donnée vers un pays étranger.

5.4 Droits des Personnes Concernées

Il existe quatre droits des personnes concernées (PC) dans la loi 18-07.

5.4.1 Droit à l'information

Le RT doit informer de manière explicite et non ambiguë les PC des éléments suivants :

- L'identité du RT et, le cas échéant, de son représentant ;
- Les finalités du traitement ;
- Toute information complémentaire pertinente, notamment sur le destinataire, l'obligation de réponse et ses conséquences, ainsi que ses droits et le transfert de données à l'étranger.

5.4.2 Droit d'accès

La PC a le droit d'obtenir du RT :

- La confirmation de l'existence ou non d'un traitement de DCP les concernant ;
- Les finalités du traitement, les catégories de données concernées et les destinataires ;
- La communication, sous une forme intelligible, des données faisant l'objet du traitement, ainsi que toute information disponible sur l'origine des données.

5.4.3 Droit de rectification

Les PC ont le droit d'obtenir la mise à jour, la rectification, l'effacement ou le blocage des DPC dont le traitement n'est pas conforme à la loi 18-07. Le RT est tenu d'effectuer les rectifications nécessaires dans les 10 jours.

5.4.3 Droit d'opposition

Les PC ont le droit de s'opposer au traitement de leurs DCP pour des motifs légitimes. Par ailleurs, ils peuvent s'opposer à l'utilisation de leurs données personnelles à des fins de prospection, notamment à des fins commerciales.

5.5 Synthèse sur la loi 18-07

Le tableau 2.2 suivant illustre une synthèse générale sur la loi 18-07 par rapport à certains critères de droit et d'éligibilité (champs d'application, transparence, responsabilité…etc.) :

Critères		Valeurs
Autorité de contrôle	Existe-t-il une autorité de contrôle ?	Oui (ANPDP), les articles de 22 à 31
Champ d'application	S'applique aux personnes physiques	Oui
	S'applique aux personnes morales	Oui
	S'applique aux entités publiques	Oui
	Exclusion des fins domestiques/personnelles	Oui

	Exclusion pour des raisons de sécurité nationale	Oui
	Exclusion à des fins journalistiques, littéraires ou artistiques	Non
	Exclusion des fonctions judiciaires	Non
Données personnelles	DCP	l'identité physique, physiologique, génétique, biométrique, psychique, économique, culturelle ou sociale
	DCP sensible	Origine ethnique ou raciale, opinions politiques, croyances religieuses ou philosophiques, appartenance syndicale, données de santé et génétiques
Transparence	Notification du traitement des données	Oui
	Notification à l'autorité nationale en cas de violation de données	Partiel
	Notification à la personne concernée en cas de violation de données	-
	Le délai de notification est spécifié	Non
	Nécessite un registre de traitement des données	Oui
Responsabilité	L'Autorité nationale est habilitée à enquêter sur	Oui
	La Loi prévoit des sanctions pénales	Oui
	La Loi prévoit des sanctions administratives	Oui
Droits des PC	Droit à l'information	Oui
	Droit d'accès	Oui
	Droit de rectification	Oui
	Droit d'opposition	Oui
Transfert transfrontalier	Transfert des données vers un pays étranger	Oui avec des conditions
Traitement automatisé	Prévoit le droit de ne pas faire l'objet d'une prise de décision automatisée	Oui

Tableau 2.2 : Synthèse sur la loi 18-07

6 Portail numérique de l'ANPDP et les organismes

L'accès au portail numérique de l'ANPDP se fait à travers l'adresse Web officielle de l'autorité nationale suivante : www.ANPDP.DZ

6.1 Les recommandations de l'ANPDP

Les recommandations de l'ANPDP pour se conformer à la loi 18-07 sont les suivantes **[11]** :

- Chaque organisme ou personne physique concerné par le traitement des DCP doit désigner son représentant habilité (RepH) ayant un profil approprié et qui prendra en charge les tâches suivantes :

- Etablir la cartographie des traitements,
- Assurer le suivi,
- Sensibiliser les utilisateurs des traitements sur les dispositions et les normes de conformité telles que mentionnées dans la loi 18-07.

Le RepH doit avoir un accès direct au premier responsable de l'organisme pour lui signaler les cas potentiels de violation de la loi 18-07. Le RepH est le point de contact de l'ANPDP.

- Chaque organisme doit installer préalablement une entité ou cellule pour, d'une part, arrêter la cartographie des traitements effectués sur les DCP (liste des traitements, lieu et procédure d'exécution de chaque traitement…), et, d'autre part, classifier chaque traitement selon le besoin d'obtention d'une déclaration ou d'une demande d'autorisation auprès de l'ANPDP.

6.2 Les application de l'ANPDP

Pour que le RT d'un organisme puisse exercer ces obligations telles qu'édictées dans la loi 18-07, il doit, en premier lieu, créer un compte utilisateur pour accéder au portail de l'autorité.

La figure 2.3 schématise le menu principal du portail numérique à travers lequel le RT peut accéder aux trois procédures suivantes **[11]** :

1. Procédure de déclaration des traitements
2. Procédure de demande des autorisations
3. Procédure de demande d'avis

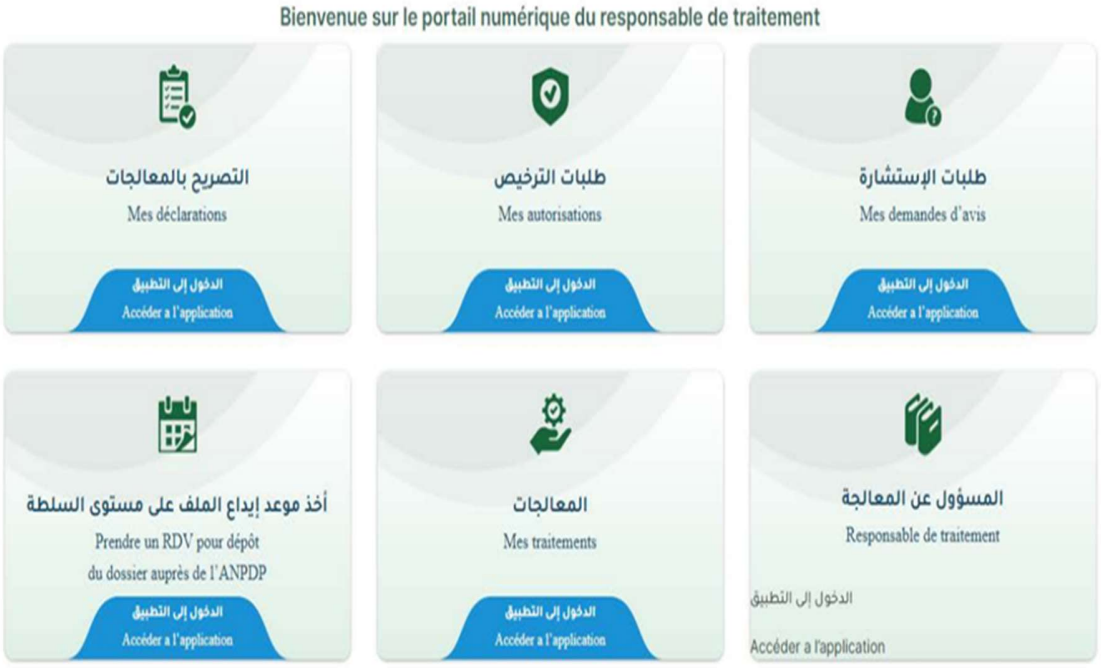


Figure 2.3 : Portail numérique du RT.

7 Conclusion

L'engagement de l'État algérien et sa prise de responsabilité pour la protection et la préservation de la vie privée des personnes s'est concrétisé en 2018 par la promulgation de la loi 18-07 portant sur « la protection des personnes physiques dans le traitement des données à caractère personnel » et de sa mise en application en 2022, suivie par la création de l'Autorité Nationale de Protection des Données à caractère Personnel (ANPDP).

À cet effet, nous avons jugé utile de consacrer entièrement le chapitre deux (02) au développement des missions, de l'organisation et du mode de fonctionnement de l'ANPDP, ainsi qu'à la présentation des sept (07) titres qui composent la loi 18-07.

Ces deux évènements s'inscrivent aussi comme axes principaux dans la feuille de route tracée par les autorités pour assurer la mutation vers la souveraineté numérique tant convoitée par l'État comme partie prenante de la souveraineté nationale.

Les concepts développés et les synthèses résultants des deux chapitres 1 & 2 représentent un préambule pour entamer l'étude conceptuelle de l'application informatique objet du chapitre n° 03 suivant.

Chapitre 3

Conceptualisation d'un outil informatique pour la protection des DCP conformément à la loi 18-07

1 Introduction

La phase de conception est une étape importante dans le cycle de développement logiciel. Elle permet de structurer, organiser et planifier le projet.

Dans ce chapitre, nous allons présenter en détails la conception du projet à travers les diagrammes de cas d'utilisation, des activités et des classes ainsi que le modèle relationnel.

2 Processus de développement

2.1 Les processus de développement généralistes

Les processus de développement ont pour rôle de guider l'équipe de développement dans la réalisation de logiciels. Il existe de nombreux processus de développement, chacun ayant ses avantages et ses inconvénients. Pour la plupart, ils sont construits autour des mêmes grandes étapes **[25]** :

- Analyse des besoins,
- Conception,
- Implémentation,
- Vérification et validation,
- Déploiement.

2.2 Le processus UP

Le processus UP (Unified Process) est un cadre de développement logiciel itératif et incrémental, comme illustré dans la figure 3.1, qui se concentre sur la production de logiciels de haute qualité tout en répondant aux besoins variables des clients, Il est conçu pour être adaptable à différents types de projets **[26]**.

Le processus UP associé à UML met en œuvre les principes suivants **[27]** :

- Processus itératif et incrémental,
- Processus guidé par les cas d'utilisation,
- Processus centré sur l'architecture,
- Processus orienté par la réduction des risques.

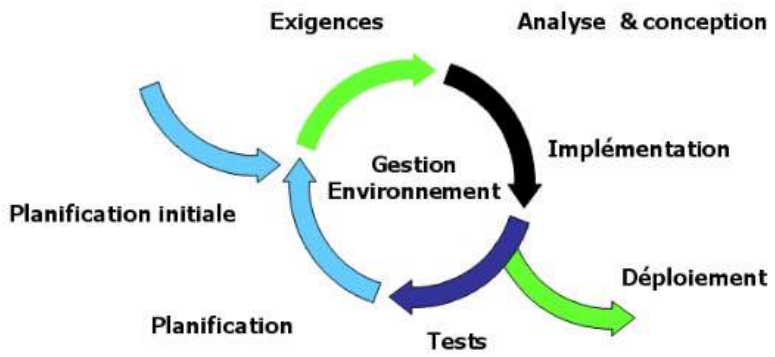


Figure 3.1 : Schéma descriptif du cycle itératif et incrémental

UP décrit qui fait quoi, comment et quand les travaux sont réalisés tout au long du cycle de vie du projet. Quatre concepts d'UP répondent à ces questions [39] :

- Rôle (qui ?) :
- Activité (comment ?)
- Artefact (quoi ?)
- Workflow (quand ?)

Pour une meilleure maitrise de notre projet, le processus UP nous décrit une démarche en deux axes, comme le montre la figure 3.2 :

A) Un axe horizontal devisé en quatre phases :

1.1 Inception (Lancement) : correspond à l'initialisation du projet où l'on mène une étude d'opportunité et de faisabilité du système à construire.

1.2 Élaboration : correspond à la validation des cas d'utilisation résultant de la phase précédente, de l'évaluation des risques et de l'étude de la rentabilité du projet ainsi qu'à la planification de la phase de construction.

1.3 Construction : correspond à la production d'une première version du produit, elle est concentrée sur les phases des activités de conception, d'implémentation et de test.

1.4 Transition : correspond à la livraison du produit pour une exploitation réelle où des « béta tests » sont effectués pour valider le nouveau système auprès des utilisateurs.

1.5 Itérations : une itération est un circuit complet de développement aboutissant à une livraison d'un produit exécutable.

B) Un axe vertical qui présente l'enchainement des activités dans le processus UP :

1. Expression des besoins : UP distingue deux types de besoins :
   - Les besoins fonctionnels qui conduisent à l'élaboration des cas d'utilisation,
   - Les besoins non fonctionnels (techniques) qui aboutissent à la rédaction d'une matrice des exigences.

2. Analyse : l'analyse se concrétise par l'élaboration de tous les diagrammes donnant une représentation du système tant statique (diagramme de classe principalement), que dynamique (diagramme des cas d'utilisation, de séquence, d'activité, d'état-transition...).

3. Conception : la conception prend en compte les choix d'architecture technique retenus pour le développement et l'exploitation du système. La conception permet d'étendre la représentation des diagrammes effectuée au niveau de l'analyse en y intégrant les aspects techniques les plus proches des préoccupations physiques.

4. Implémentation : Cette phase correspond à la production du logiciel sous forme de composants, de bibliothèques ou de fichiers.

5. Test : Les tests permettent de vérifier :
   - la bonne implémentation de toutes les exigences (fonctionnelles et techniques),
   - le fonctionnement correct des interactions entre les objets,
   - la bonne intégration de tous les composants dans le logiciel.

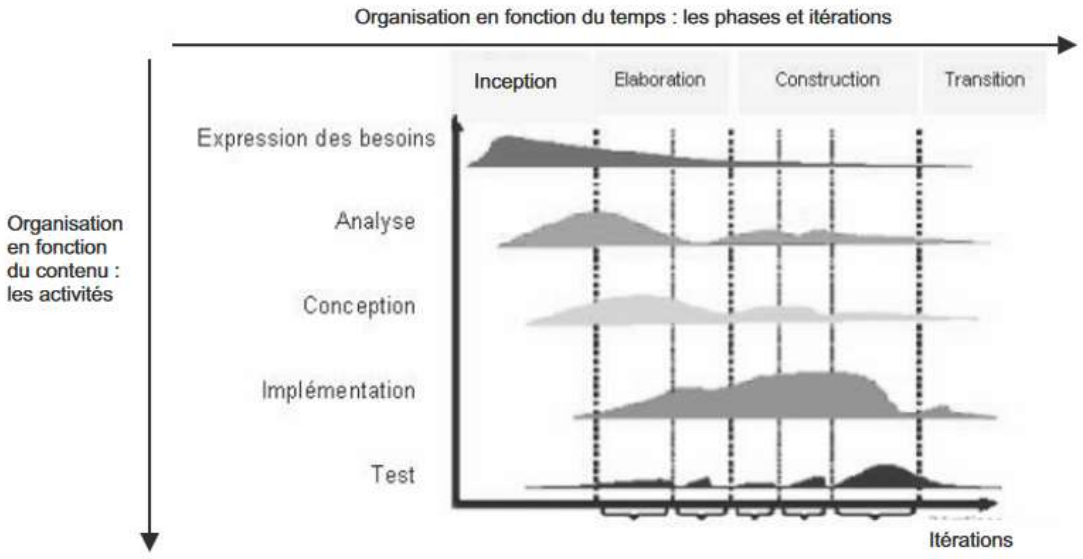


Figure 3.2 : Schéma d'ensemble du processus UP (source : [**27**])

3 Conceptualisation

3.1 Étude préliminaire

L'étude préliminaire a pour objectifs principaux de **[39]** :

- établir un recueil initial des besoins fonctionnels et opérationnels,
- modéliser le contexte du système.

3.1.1 Besoins fonctionnels et opérationnels

Les besoins fonctionnels représentent les fonctionnalités principales du système **[40]**.

Besoins	Fonctionnalités
Gestion du registre des traitements des DCP	Le RT suit le traitement dans l'application. Le RepH vérifie la validité du traitement par rapport à la loi 18-07 et suit la déclaration soumise à l'ANPDP.
Gestion des droits des PC	Le RepH suit la demande de droit de la PC et notifie les résultats aux tiers. Le RT traite la demande de droit.
Gestion des violations des DCP	Le RepH suit la violation des DCP dans l'application, il élabore le plan d'action des mesures préventives, notifie les tiers et clôture le dossier. Le RSSI traite la violation et.
Administration de la BD	L'administrateur : - Contrôle l'accès à toutes les fonctionnalités, - Gère la BD, - Sauvegarde et restaure la BD. - Crée et modifie le profil utilisateur.
Authentification et accès	L'utilisateur doit entrer un mot de passe pour accéder à l'application.

Tableau 3.1 : Besoins fonctionnels du système

Les besoins non fonctionnels sont des indicateurs de qualité de l'exécution des besoins fonctionnels **[40]**. Dans notre cas, ils se traduisent en les trois (03) points suivants:

1. Sécurité :
    - L'administrateur système est chargé de définir les profils des utilisateurs,
    - Les mots de passe sont stockés de manière sécurisée.

2. Educatif :
    - Assurer une passerelle informative entre les opérations du système d'une part et l'essence juridique de la loi 18-07 d'autre part.

3 Ergonomie :

- Intégrer des textes d'infobulle dans l'application afin d'aider les utilisateurs à naviguer et à interagir avec l'application de manière efficace.

3.1.2 Diagramme de contexte

Le diagramme de contexte dynamique de notre application « Conform1807 » est illustré dans la figure 3.3, on ressort avec les acteurs identifiés du système :

1. Acteurs principaux :
    - Le RT,
    - Le RepH,
    - Le RSSI,
    - L'administrateur.
2. Acteurs secondaires :
    - La PC,
    - L'ANPDP.

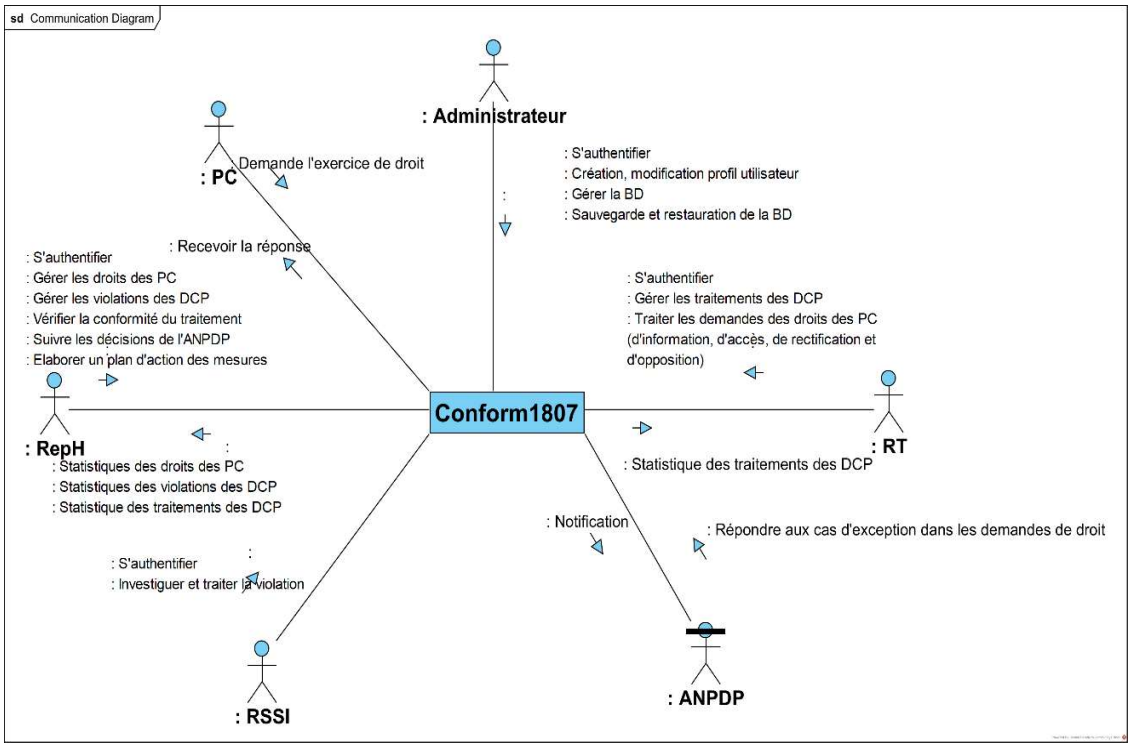


Figure 3.3 : Diagramme de contexte dynamique de « Conform1807 »

Un package UML représente un espace de nommage qui peut contenir **[40]** :

- Des éléments d'un modèle,
- Des diagrammes qui représentent les éléments du modèle,
- D'autres packages.

Si nous considérons le diagramme de contexte dynamique de la figure 3.3 et en affectant chaque cas d'utilisation à un package, nous obtenons la répartition suivante :

Cas d'utilisation	Acteurs	Package
Suivre le traitement des DCP	RT	Gestion des traitements des DCP
Vérifier la conformité du traitement des DCP	RepH	
Suivre les décisions de l'ANPDP	RepH	
	ANPDP	
Suivre la demande de droit des PC	RepH	Gestion des demandes de droits des PC
	PC	
Traiter la demande de droit des PC	RT	
	ANPDP	
Suivre la violation des DCP	RepH	Gestion des violations des DCP
	ANPDP	
	PC	
Traiter la violation des DCP	RSSI	
Gérer les utilisateurs	Administrateur	Service support
Gérer la BD		

Tableau 3.2 : Répartition des cas d'utilisation et acteurs par package

3.2 Élaboration du diagramme de cas d'utilisation

Le Diagramme de Cas d'Utilisation (DCU) est présenté dans la figure 3.4 où on identifie quatre acteurs principaux et deux acteurs secondaires :

- Acteurs principaux : le RT, le RepH, le RSSI et l'administrateur.
- Acteurs secondaires : l'ANPDP et la PC.

À chaque cas d'utilisation doit être associée une description textuelle des interactions entre l'acteur et le système et les actions que le système doit réaliser en vue de produire les résultats attendus par les acteurs **[27] [28].**

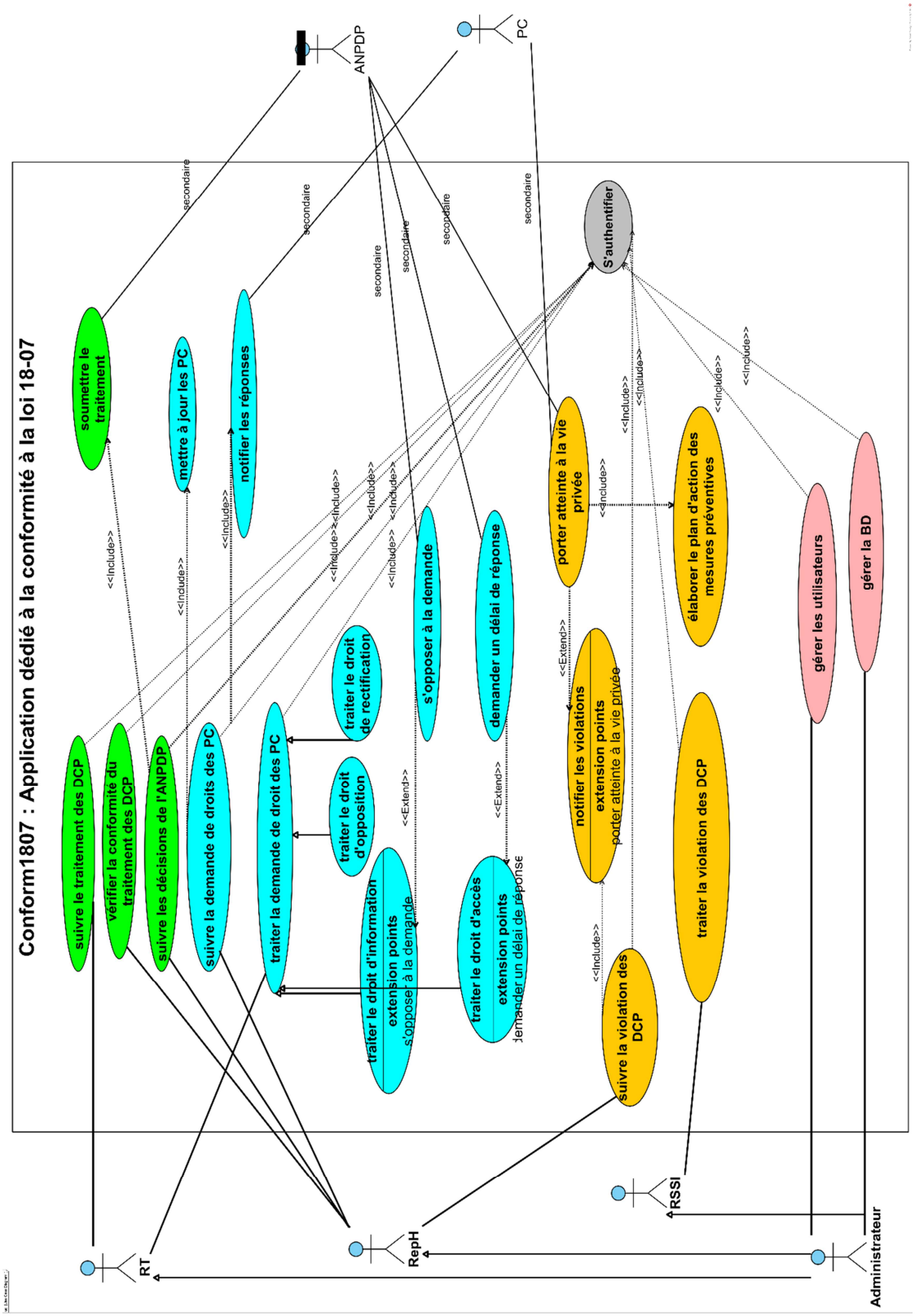


Figure 3.4 : Diagramme de cas d'utilisation de notre application

La description textuelle du cas d'utilisation « S'authentifier » est décrite dans le tableau 3.1.

Cas d'utilisation 0	**S'authentifier.**
Objectif	Permettre l'accès à l'application
Acteurs concernés	Administrateur, RepH, RT et RSSI.
Préconditions	Aucune
Post conditions	Aucune
Scénario nominal	1. L'utilisateur choisit le nom utilisateur (Login) dans la liste déroulante. 2. L'utilisateur est demandé d'introduire son mot de passe (la première fois). 3. L'utilisateur saisit le mot de passe, s'il existe déjà. 4. Le système valide la saisie de l'utilisateur. 5. L'utilisateur accède à l'application.
Scénarios alternatifs	4-a : Erreurs dans la saisie du login ou du mot de passe : - Le système informe l'utilisateur que le login ou le mot de passe est erroné. - L'utilisateur choisit le nom utilisateur correct et retape le mot de passe. - Retour à l'action 4 du scénario nominal. 4-b : Erreur dans la saisie du mot de passe pour la première fois (création) : - Le système rappelle les critères de création du mot de passe (longueur minimale de 12 caractères, au moins un caractère alphabétique, un caractère numérique et un caractère spécial). - Retour à l'action 4 du scénario nominal. 4-c : Cas d'oubli du mot de passe : - L'utilisateur contacte l'administrateur pour appliquer la procédure de recouvrement du mot de passe.

Tableau 3.3 : Description du cas d'utilisation « S'authentifier »

La description textuelle du cas d'utilisation «Suivre le traitement des DCP » est décrite dans le tableau 3.4.

Cas d'utilisation 1	**Suivre le traitement des DCP**
Objectif	Mettre à jour le registre des traitements des DCP
Acteurs concernés	RT
Préconditions	Le RT s'est authentifié correctement à l'application.
Post conditions	Aucune

Scénario nominal	1. Le RT ajoute un nouveau traitement dans le registre des traitements des DCP. 2. Le RT saisit l'identification générale du traitement ainsi que les autres types d'information : Sous-traitement, les sous-traitants, les destinataires, les catégories des données collectées, les services des droits des PC les responsables. 3. Le système valide la saisie. 4. Le RT sauvegarde le traitement. 5. Le RT demande au RepH de valider le traitement en positionnant l'état de l'enregistrement dans : attente validation. 6. Le RT verrouille le traitement après sa validation par le RepH.
Scénarios alternatifs	2-a : Erreur dans la saisie des données du traitement : - Le système réaffiche le formulaire de saisie en pointant les erreurs détectées. - Le RT corrige les erreurs. - Le cas d'utilisation reprend à l'action 2 du scénario nominal.

Tableau 3.4 : Description du cas d'utilisation « Suivre le traitement des DCP »

La description textuelle du cas d'utilisation «Vérifier la conformité du traitement des DCP » est décrite dans le tableau 3.5.

Cas d'utilisation 2	**Vérifier la conformité du traitement des DCP**
Objectif	Vérifier que le traitement est conforme aux exigences de la loi 18-07.
Acteurs concernés	RepH
Préconditions	Le RepH s'est authentifié correctement à l'application. Le traitement a été saisi par le RT.
Post conditions	Aucune
Scénario nominal	1. Le RepH cherche le traitement dans l'application. 2. Le RepH vérifie la conformité du traitement. 3. Le RepH valide le traitement.
Scénarios alternatifs	

Tableau 3.5 : Description du cas d'utilisation « Vérifier la conformité du traitement des DCP »

La description textuelle du cas d'utilisation « Suivre les décisions de l'ANPDP » est décrite dans le tableau 3.6.

Cas d'utilisation 3	**Suivre les décisions de l'ANPDP**
Objectif	Suivre les déclarations du traitement soumis à l'ANPDP.
Acteurs concernés	RepH et l'ANPDP (secondaire)
Préconditions	Le RepH s'est authentifié correctement à l'application. Le traitement a été bien saisi par le RT. Le RepH est un compte d'accès au portail Web de l'ANPDP.
Post conditions	Aucune
Scénario nominal	1. Le RepH cherche le traitement dans l'application. 2. Le RepH accède au portail Web de l'ANPDP. 3. Le RepH saisit la déclaration du traitement. 4. Le RepH imprime et soumet la déclaration du traitement à l'ANPDP. 5. Le RepH reçoit la validation du traitement par l'ANPDP. 6. Le RepH met à jour le registre des traitements.
Scénarios alternatifs	

Tableau 3.6 : Description du cas d'utilisation «Suivre les décisions de l'ANPDP »

La description textuelle du cas d'utilisation « Suivre la demande de droit des PC » est décrite dans le tableau 3.7.

Cas d'utilisation 4	**Suivre la demande de droit des PC**
Objectif	Mettre à jour le registre des demandes de droit des PC.
Acteurs concernés	RepH, PC
Préconditions	Le RepH s'est authentifié correctement à l'application. L'existence d'une base de données des traitements des DCP.
Post conditions	Aucune
Scénario nominal	1. Le RepH reçoit la demande de la PC. 2. Le RepH introduit la PC dans l'application s'il n'existe pas. 3. Le RepH introduit la demande de droit de la PC dans l'application. 4. Le RepH identifie la PC et le service facilitant l'exercice de droit dans l'application. 5. Le RepH analyse la demande. 6. Le RepH attend le traitement de la demande par le RT. 7. Le RepH notifie la PC des résultats du traitement.

	8. Le RepH notifie le RT de la clôture de la demande.
Scénarios alternatifs	4-a : Erreur, la PC n'est pas introduite dans l'application : - Le cas d'utilisation reprend à l'action 2 du scénario nominal.

Tableau 3.7 : Description du cas d'utilisation « Suivre la demande de droit des PC »

La description textuelle du cas d'utilisation «Traiter la demande de droit des PC » est décrite dans le tableau 3.8.

Cas d'utilisation 5	**Traiter la demande de droit des PC**
Objectif	Mettre à jour le registre des demandes de droit des PC.
Acteurs concernés	RT et ANPDP
Préconditions	Le RT s'est authentifié correctement à l'application. Le RepH a introduit la demande dans l'application.
Post conditions	Aucune
Scénario nominal	1. Le RT recherche la demande dans l'application. 2. Le RT traite la demande de droit de la PC dans l'application.
Scénarios alternatifs	

Tableau 3.8 : Description du cas d'utilisation «Traiter la demande de droit des PC »

La description textuelle du cas d'utilisation « Suivre la violation des DCP » est décrite dans le tableau 3.9.

Cas d'utilisation 6	**Suivre la violations des DCP**
Objectif	Mettre à jour le registre des violations des DCP et élabore un plan d'action des mesures préventives.
Acteurs concernés	RepH, RT, PC et ANPDP
Préconditions	Le RepH s'est authentifié correctement à l'application.
Post conditions	Aucune
Scénario nominal	1. Le RepH reçoit le rapport d'identification de la violation du RSSI. 2. Le RepH crée un nouvel enregistrement dans l'application. 3. Le RepH saisit dans l'application le rapport de la violation. 4. Le système valide la saisie.

	5. Le RepH demande le traitement de la violation en positionnant l'état de l'enregistrement dans « en attente de traitement ». 6. Le RepH documente la demande, communique les notifications aux tiers.
Scénarios alternatifs	Aucune

Tableau 3.9 : Description du cas d'utilisation « Suivre la violation des DCP »

La description textuelle du cas d'utilisation « Traite la violation des DCP » est décrite dans le tableau 3.10.

Cas d'utilisation 7	**Traite la violations des DCP**
Objectif	Traiter la violation des DCP
Acteurs concernés	RSSI
Préconditions	Le RSSI s'est authentifié correctement à l'application.
Post conditions	Aucune
Scénario nominal	1. Le RSSI cherche l'enregistrement de la violation dans l'application. 2. Le RSSI saisit le traitement de la violation. 3. Le système valide la saisie. 4. Le RSSI positionne l'état de l'enregistrement dans « résolu ».
Scénarios alternatifs	Aucune

Tableau 3.10 : Description du cas d'utilisation « Traite la violation des DCP »

La description textuelle du cas d'utilisation « Gérer les utilisateurs » est décrite dans le tableau 3.11.

Cas d'utilisation 8	**Gérer les utilisateurs**
Objectif	Mise à jour des utilisateurs et leurs rôles dans le système.
Acteurs concernés	Administrateur.
Préconditions	L'administrateur s'est authentifié correctement à l'application.
Post conditions	Aucune
Scénario nominal	1. L'administrateur clique sur le bouton « Administrer la base de données ». 2. Le système affiche un panneau qui contient trois boutons. 3. L'administrateur choisit le bouton « Gestion des utilisateurs ».

	4. Le système affiche un panneau qui contient deux boutons à savoir : M.A.J. utilisateurs et rôles. 5. L'administrateur choisit le bouton « M.A.J. Utilisateurs ». 6. Le système affiche le programme « M.A.J. Utilisateurs ». 7. L'utilisateur ajoute un nouvel utilisateur. 8. L'utilisateur saisit les informations de l'utilisateur. 9. Le système valide la saisie. 10. L'utilisateur clique sur le bouton « Enregistrer ».
Scénarios alternatifs	8-a : Erreur dans la saisie du nouvel utilisateur : - L'utilisateur corrige les erreurs. - Le cas d'utilisation reprend à l'action 8 du scénario nominal.

Tableau 3.11 : Description du cas d'utilisation « Gérer les utilisateurs »

La description textuelle du cas d'utilisation « Gérer la BD » est décrite dans le tableau 3.12.

Cas d'utilisation 9	**Gérer la BD**
Objectif	Mise à jour des tables de base du système, sauvegarde et restauration (RT, RepH, RSSI, catégories des données, catégories des PC).
Acteurs concernés	Administrateur.
Préconditions	L'administrateur s'est authentifié correctement à l'application.
Post conditions	Aucune
Scénario nominal	1. L'administrateur clique sur le bouton « Administrer la base de données ». 2. Le système affiche un panneau qui contient trois boutons. 3. L'administrateur choisit le bouton « M.A.J. Tables de base ». 4. Le système affiche un panneau qui contient six boutons. 5. L'administrateur choisit le bouton « Table catégorie des données ». 6. Le système affiche le programme « M.A.J. Table catégorie des données ». 7. L'utilisateur ajoute une nouvelle catégorie de données. 8. Le système valide la saisie. 9. L'utilisateur clique sur le bouton « Enregistrer ».

Scénarios alternatifs	8-a : Erreur, une information obligatoire n'est pas saisie : - L'utilisateur corrige l'erreur. - Le cas d'utilisation reprend à l'action 8 du scénario nominal.

Tableau 3.12 : Description du cas d'utilisation « Gérer la BD »

3.3 Élaboration du diagramme d'activité (DAC)

L'étude préliminaire des besoins fonctionnels et opérationnels a fait ressortir que notre système sera basé sur trois activités principales dont nous décrivons les diagrammes comme suit :

1. DAC du package « Gestion des traitements des DCP »

   Dans ce digramme, on a deux acteurs principaux et un acteur secondaire, comme illustré dans la figure 3.5 :

   a) Le RT, acteur principal, suit le traitement des DCP.
   b) Le RepH, acteur principal, vérifie la conformité du traitement par rapport à la loi 18-07 et imprime la déclaration du traitement à soumettre à l'ANPDP à travers le portail Web.
   c) L'ANPDP, acteur secondaire, reçoit la déclaration du traitement.

2. DAC du module « Gestion des demandes droits des PC »

   Dans ce diagramme, on a deux acteurs principaux et deux acteurs secondaires, comme illustré dans la figure 3.6 :

   a) Le RepH, un acteur principal, reçoit la demande des droits de la PC et suit la demande des droits. Il documente et notifie aux tiers les résultats.
   b) Le RT, acteur principal, traite la demande des droits des PC.
   c) La PC, acteur secondaire, demande l'exercice de ces droits.
   d) L'ANPDP, acteur secondaire, répond aux demandes de délai de réponse.

3. DAC du package « Gestion des violations des DCP »

   Dans ce diagramme, on a deux acteurs principaux et deux acteurs secondaires, comme illustré dans la figure 3.7 :

   a) Le RepH, acteur principal, suit la violation des DCP. Il notifie aux tiers la violation.
   b) Le RSSI, acteur principal, envoie le rapport de détection de la violation des DCP au RepH et traite la violation et élabore le plan d'action des mesures préventives.
   c) L'ANPDP et la PC, acteurs secondaires, reçoivent les notifications de violations.

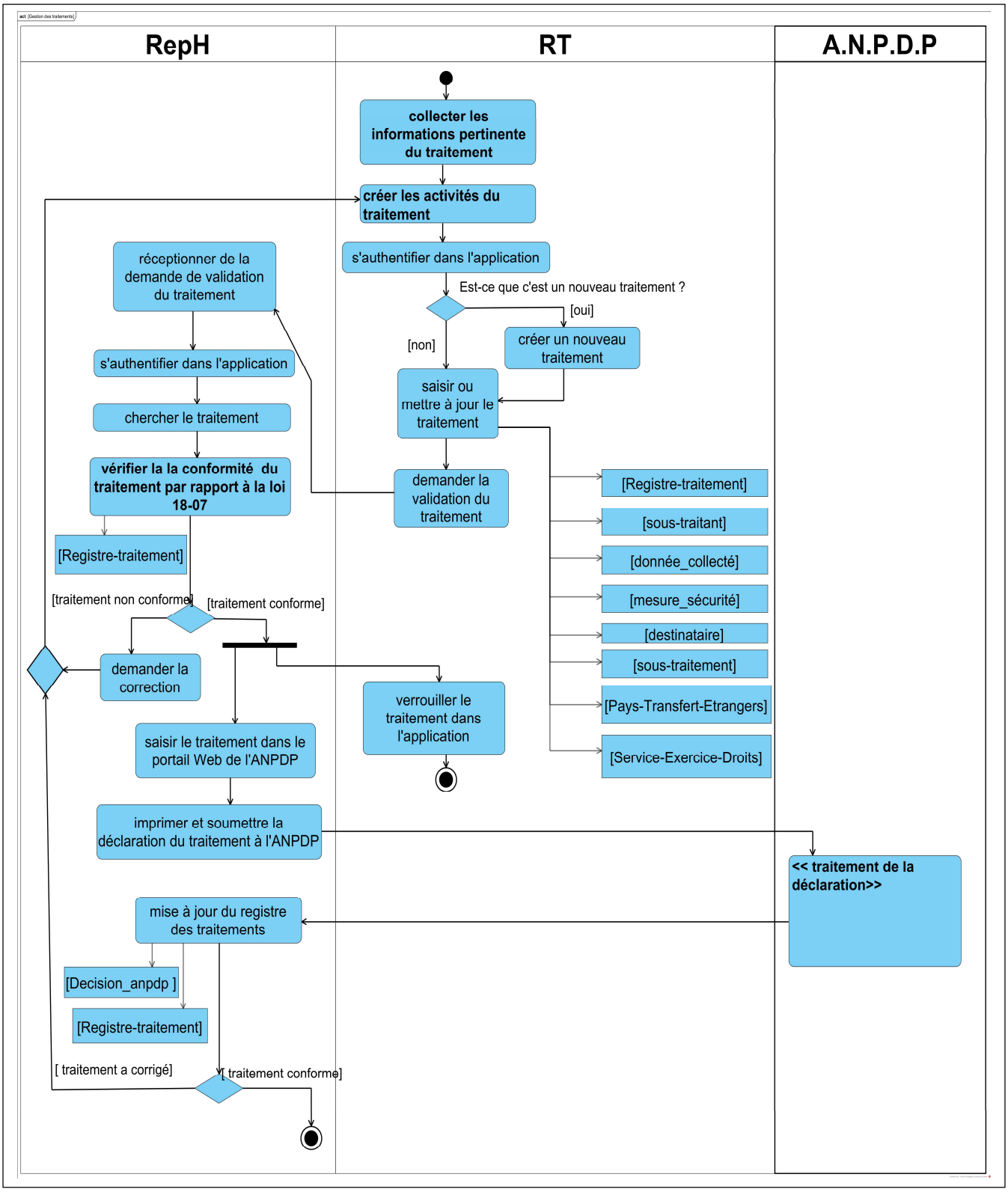


Figure 3.5 : DAC du package « Gestion des traitements des DCP »

Le DAC du module « Gestion des demande de droits des PC » est décrit dans la figure 3.6.

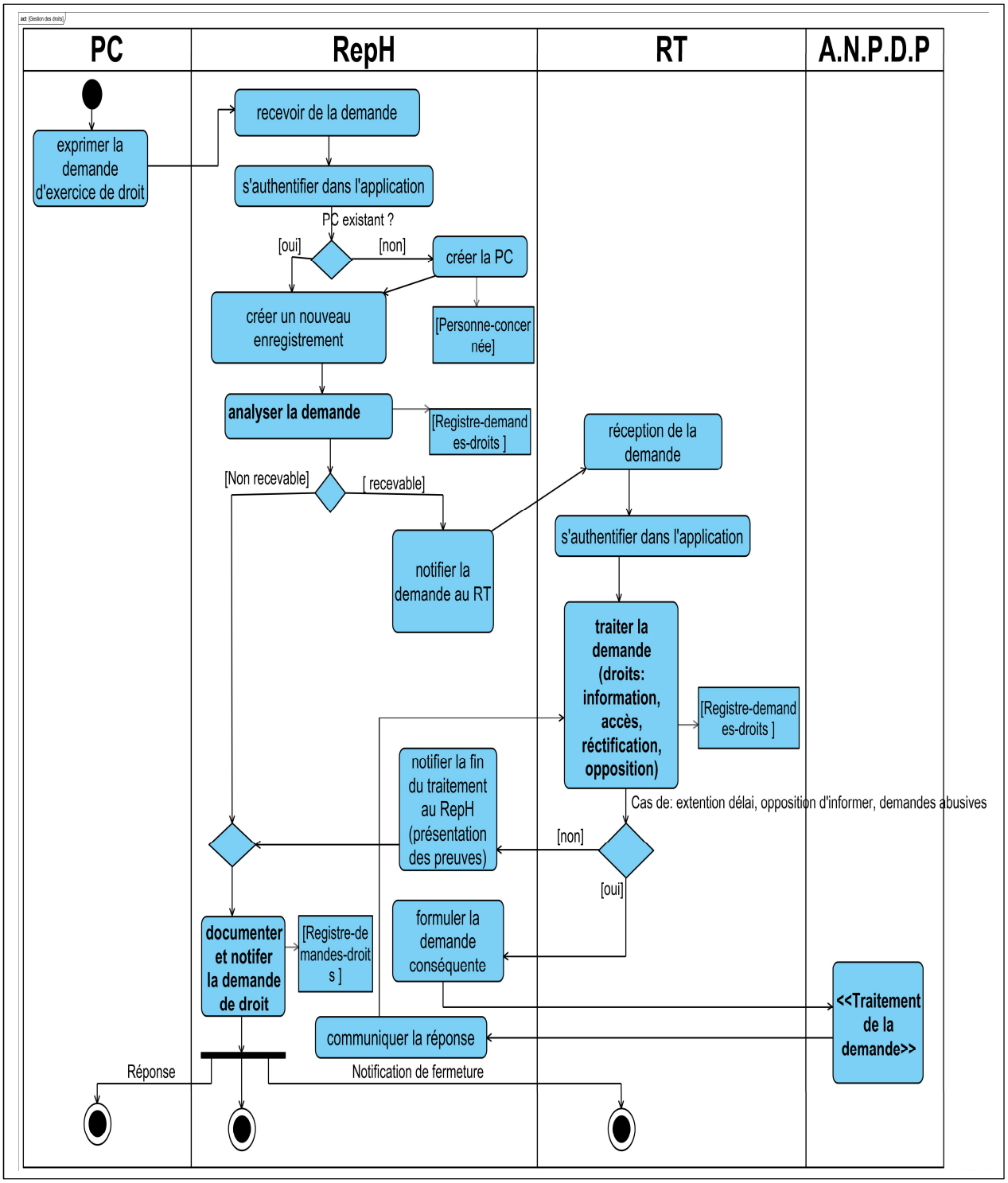


Figure 3.6 : DAC du package « Gestion des demandes de droits des PC »

Le DAC du module « Gestion des violations des DCP » est décrit dans la figure 3.7.

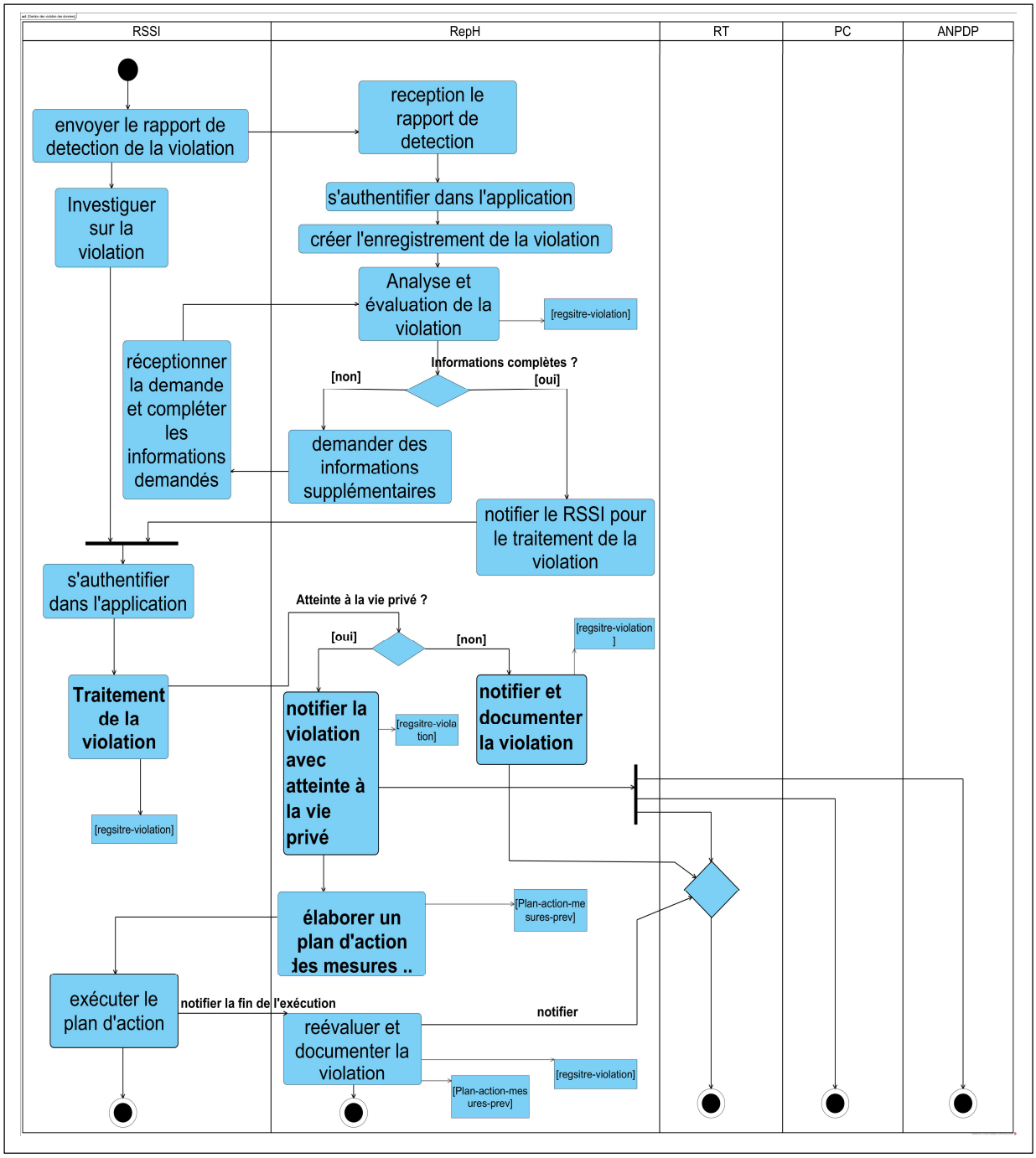


Figure 3.7 : DAC du package « Gestion des violations des DCP »

3.4 Élaboration du diagramme de classe

Le diagramme de classe (DCL) est une représentation statique des éléments qui composent un système et de leurs relations **[43]**. Le DCL de notre application est représenté dans la figure 3.8.

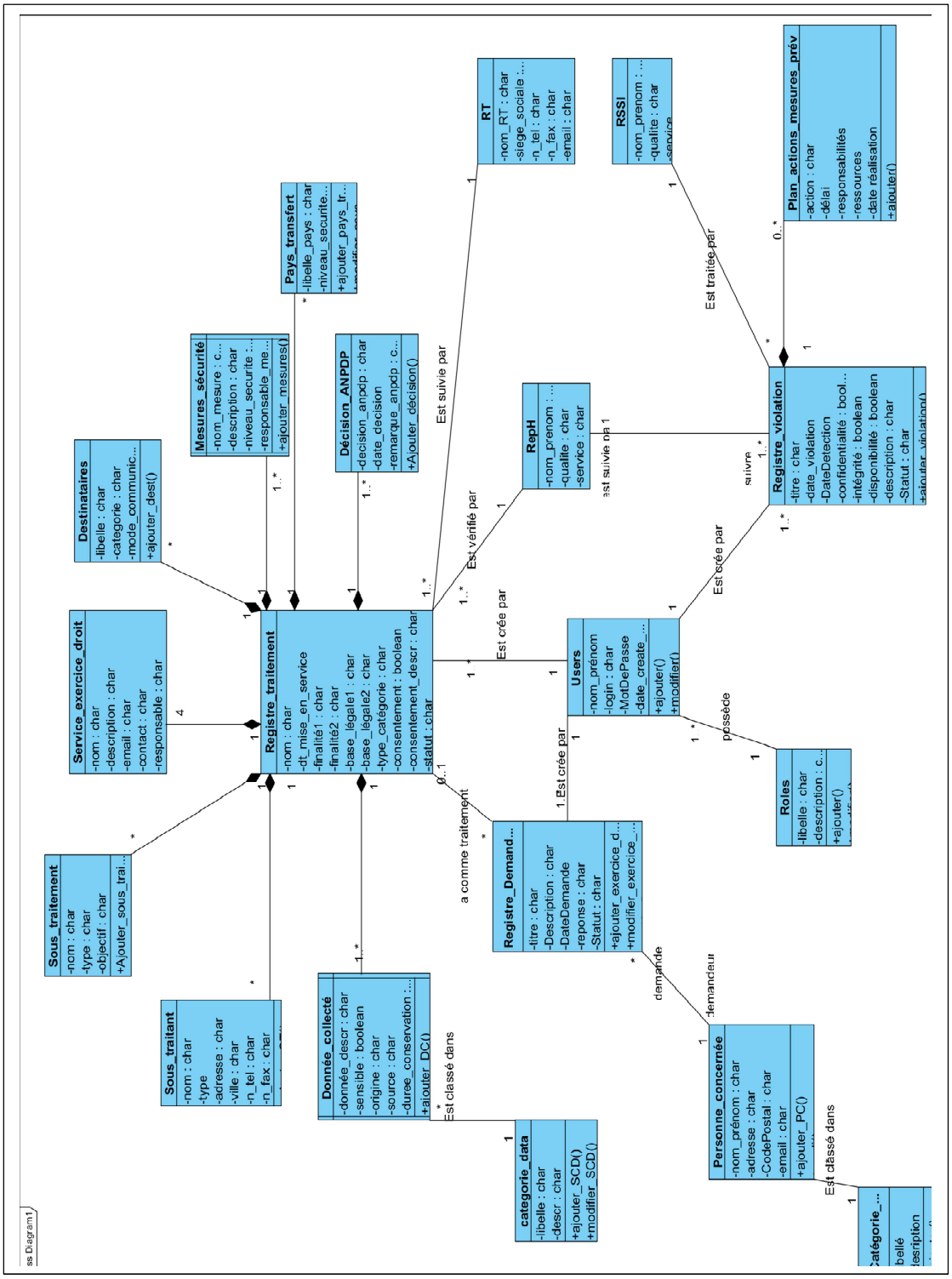


Figure 3.8 : Diagramme de classe du système

4 Systèmes de gestion des bases de données

4.1 Base de données

Une Base de données (BD) est un gros ensemble d'informations structurées et mémorisées sur un support permanent **[24]**. Elle est utilisée par les organisations comme méthode de stockage, de gestion et de récupération de l'information **[29]**.

4.2 Système de gestion de base de données (SGBD)

Un SGBD est un logiciel de haut niveau qui permet de manipuler les informations stockées dans une base de données [24]. Le SGBD agit comme une interface entre les programmes d'application et les fichiers de données physiques. Les principales fonctions d'un SGBD sont les suivantes **[29]** :

1. Maintenir l'intégrité des données : réduire et éliminer la redondance des données et maximiser la cohérence des données.
2. Stockage des données : veiller à ce que les données stockées soient conformes aux données saisies.
3. Dictionnaire des données : gérer les éléments de la BD et comment ils sont liés à d'autres données via SQL.
4. Transformation et présentation des données : convertir les données saisies en format logique dans une structure et un format physique.
5. Assurer la sécurité et la confidentialité des données.
6. Autoriser le partage des données, permettant à plusieurs utilisateurs de modifier des données quasiment en même temps tout en assurant la cohérence des données.
7. Fourniture de procédures de sauvegarde et de récupération : permettre aux BD existantes d'être sauvegardées et récupérées.
8. Fournir un accès linguistique et une programmation : fournir SQL pour DBA afin de manipuler et schématiser la BD.
9. Fournit une interface pour la communication : faciliter la communication entre les BD et les autres outils.
10. Gestion des transactions : fournir les mécanismes de gestion des transactions et des commandes pour assurer la cohérence des données.

Certains SGBD populaires utilisés dans le développement d'applications comprennent Oracle, MySQL, Microsoft SQL Server, PostgreSQL et MongoDB.

4.3 Base de données de l'application

A partir du diagramme de classes décrit dans la figure 3.8, il existe des règles utilisées pour le passage du modèle du domaine vers le modèle relationnel [41] :

- Transformation des classes (R1),
- Transformation des associations un-à-plusieurs (R2),
- Transformation des associations plusieurs-à-plusieurs et n-aires (R3),
- Transformation des associations un-à-un (R4),
- Transformations des agrégations.

Après avoir appliqué les règles de passage au modèle relationnel, nous avons obtenu le schéma de la BD suivant :

Utilisateur (Id_User, Id_Rôle#, Username, Email, Password, DateCreatPwd)
Rôle (Id_Rôle, NomRole)
RT (Id_RT, Nom, Adresse, NumeroTel, Email, Fax)
RSSI (Id_RSSI, NomPrénom, DateInstallation, Actif, NumeroTel, Email, DateInstallation)
RepH (Id_RepH, NomPrénom, NumeroTel, Email, Actif, DateInstallation)
Catégorie-data (Id_CD, Catégorie, Description)
Registre-traitement (Id_RegTR, Id_RT#, Id_RepH#, Id_User#, Nom, Date, Type, Finalite1, Statut, …..)
Destinataire (Id_Dest, Id_RegTR#, Nom, Type,…)
Sous-traitement (Id_Sous_TR, Id_RegTR#, Nom, Type,…)
Sous-traitant (Id_ST, Id_RegTR#, Nom, Type, Adresse, Téléphone, Email, Fax)
Donnée-collecté (Id_DC, Id_RegTR#, Id_CD#, DataDescr, Sensible, Conservation,…)
Mesure-sécurité (Id_MS, Id_RegTR#, Nom, Type, Description, URLMesure, …)
Service-exercice-droits (Id_SED, Id_RegTR#, Nom, Type, Description, Procédure, …)
Pays-transfert-étrangers (Id_PTE, Id_RegTR#, Nom, NiveauSécurité, …)
Decision_anpdp (Id_Decsion, Id_RegTR#, DateDecision, TypeDecsion,)
Registre-demandes-droits (Id_RegDD, Titre, Description, DateDemande, TypeDemande, Id_RegTR#, ID_PC#, Id_User#, Statut, Réponse, DateRéponse, …)
Personne-concernée (Id_PC, Id_CPC#, NomPrénom, Adresse, Téléphone, Fax, Email, …)
Catégorie-personne-concernée (Id_CPC, Nom, Description)
Registre-violation (Id_RegV, Description, DateViolation, DateDetection, Id_RT#, Id_RepH#, Id_User#, Id_RSSI#, Statut, ….)
Plan-action-mesures-prev (Id_PAMP, Id_RegV#, Nom, Classe, Description, Responsable, Délai, DateRéalisation, ….)

Le schéma la base de données relationnelle est implémenté par l'utilisation de Database Designer de Microsoft Visual FoxPro V 9.0, comme illustré dans la figure 3.9.

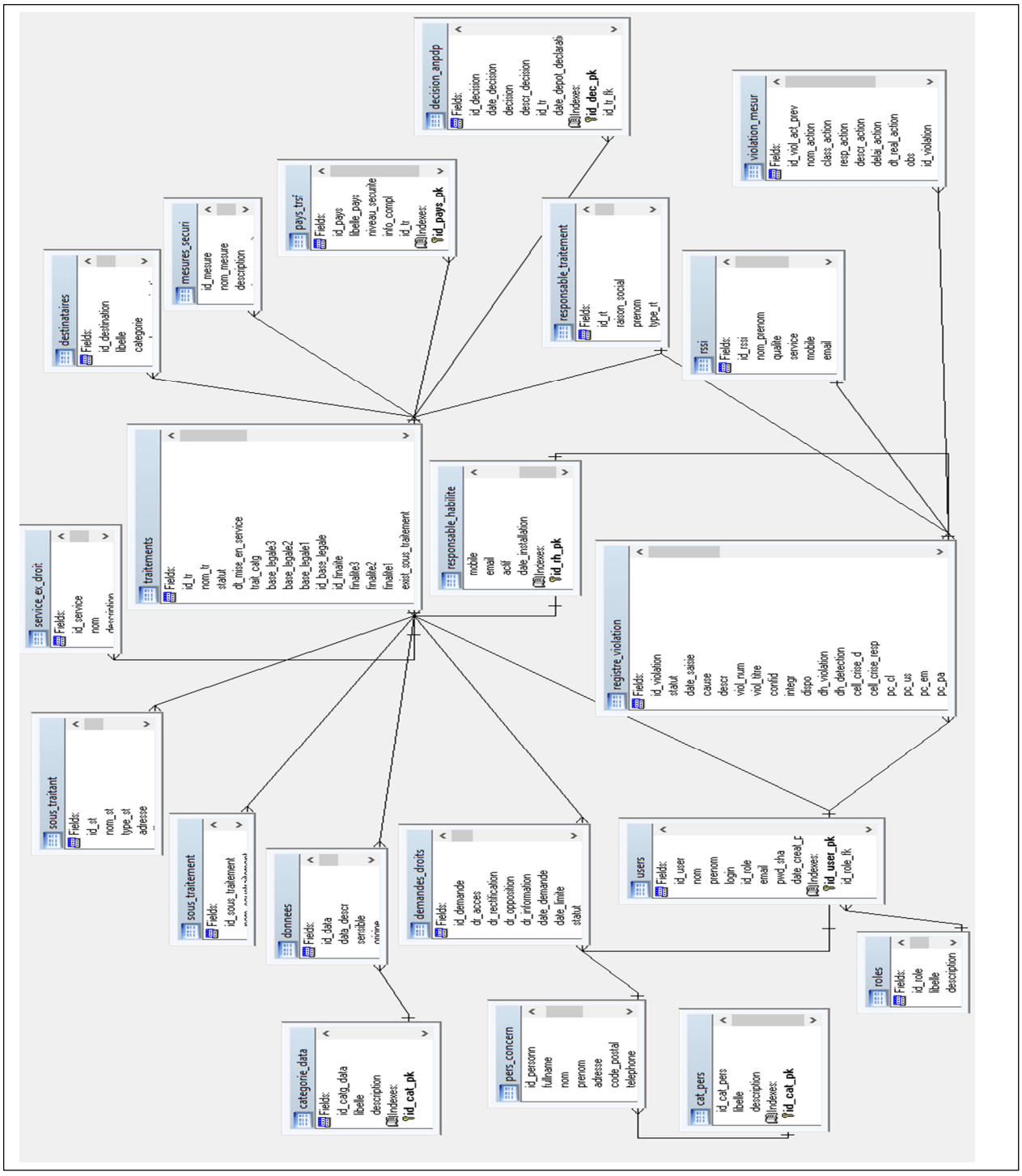


Figure 3.9 : Schéma de la BD « Conform1807 »

5 Cryptographie

La cryptologie est définie comme la « science du secret ». Longtemps concentrée sur la problématique de la confidentialité, la cryptologie a bénéficié d'un essor scientifique important suite au développement de la Société de l'information jusqu'à devenir un outil incontournable pour sécuriser les systèmes d'information **[30]**.

La cryptologie ne se limite plus aujourd'hui à assurer la **confidentialité** des secrets (figure 3.10). Elle s'est élargie au fait d'assurer mathématiquement d'autres notions : assurer **l'authenticité** d'un message (qui a envoyé ce message ?) Ou encore assurer son **intégrité** (est-ce qu'il a été modifié ?) **[4]**

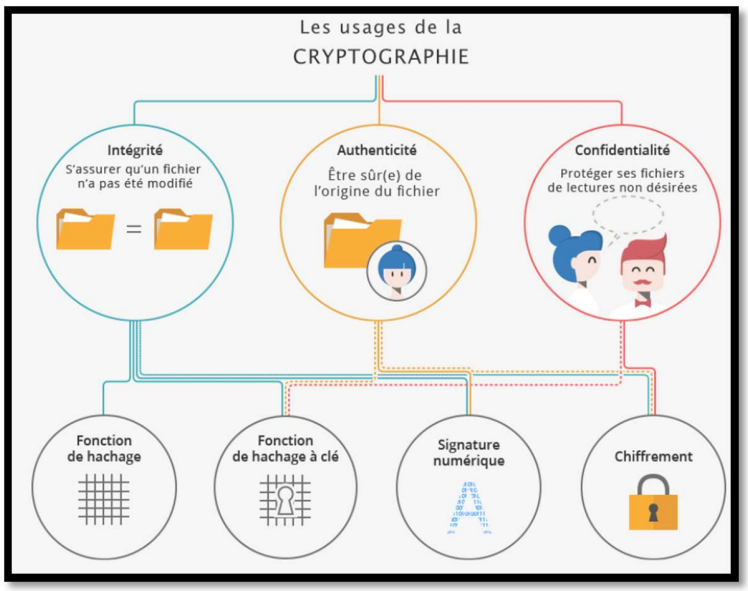


Figure 3.10 : L'usage de la cryptographie

5.1 Chiffrement

Le chiffrement **[4]** est un processus qui transforme les données en clair en données chiffrées à l'aide d'un **algorithme** et **d'une clé**. Il est souvent utilisé pour protéger la confidentialité des données lors de leur transmission ou de leur stockage. Il existe deux types de chiffrement :

a. **Chiffrement symétrique** : le chiffrement symétrique permet de chiffrer et de déchiffrer un fichier avec la même clé dite secrète. Pour s'échanger un message, il faut donc que les deux parties partagent la même clé.
b. **Chiffrement asymétrique** : le chiffrement asymétrique repose sur l'utilisation d'une paire de clés : une publique et une privée. La clé publique

est utilisée pour chiffrer les fichiers. Seule la clé privée permet de déchiffrer ces fichiers.

5.2 Hachage

Le hachage est un processus de transformation de données en une empreinte numérique unique de taille fixe, appelée hash. Cette empreinte numérique est générée à l'aide d'une fonction de hachage, qui prend en entrée des données de taille variable et produit une sortie de taille fixe. Les fonctions de hachage utilisent des mécanismes similaires aux algorithmes de chiffrement (Figure 3.11). C'est le cas pour beaucoup de fonctions de hachage comme MD4, MD5, SHA-1, SHA-2, SHA-3, etc**. [31]**.

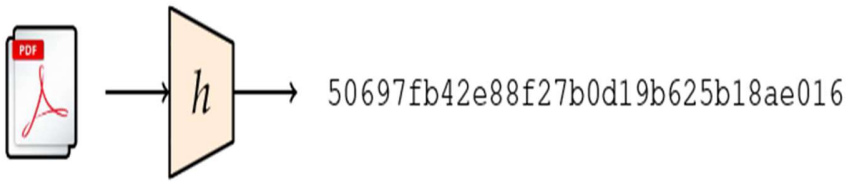


Figure 3.11 : Fonction de hachage

Pour stocker les mots de passe en sécurité, les fonctions de hachage cryptographiques telles que SHA-1, SHA-256, SHA-512, SHA3, MD5... sont conçues pour être rapides, résistantes aux collisions et aux attaques par pré-image **[32]**.

Dans notre application, nous avons implémenté l'algorithme de hachage SHA-256 pour sécuriser les mots de passe des utilisateurs, comme illustré dans la figure 3.12.

Users

ID user	Login	Id_role	Pwd_sha	Date création PWD
1	Rguettal	1	53d98ea83fd2ff44cf8f67f913a447c1d8ee347bf93d967540a55f8ba8aa46fe	05/02/24
7	Abensaci	3	82ada6e837e28469a69918a4512a28b741507d63b0e2c0e3f63efb3b1a239af1	06/11/24

Figure 3.12 : Table « users » avec le champ du mot de passe (Pwd_sha) haché

5.3 Politique de sécurité des mots de passe

Pour la politique de sécurité dans notre application, nous nous sommes focalisés sur la gestion des mots de passe en premier lieu, dont la sélection doit répondre aux critères de complexité suivants **[33]** :

1. **Longueur des mots de passe :** la taille du mot de passe doit être supérieure ou égale à 12 caractères.

2. **Règles de complexité des mots de passe :** le jeu de caractères composé d'un caractère alphabétique, d'un caractère numérique et d'un caractère spécial parmi cette liste (*, $, @, &).
3. **Stockage des mots de passe :** le stockage des mots de passe est assuré par la fonction de hachage cryptographique SHA256.
4. **Délai d'expiration des mots de passe :** le délai de renouvellement fixé pour les comptes à privilèges à six mois.
5. **Recouvrement d'un accès :** une procédure de réinitialisation du mot de passe est implémentée pour pallier l'oubli ou l'expiration d'un mot de passe. Un mécanisme de recouvrement d'accès doit être mis en place.

Cette politique est intégralement mise en œuvre dans notre application.

6 Mesures techniques et organisationnelles

Selon la loi 18-07, le RT doit mettre en œuvre des mesures de sécurité techniques et organisationnelles appropriées pour protéger les données personnelles contre la destruction accidentelle ou illicite ou la perte accidentelle, l'altération, la divulgation ou l'accès non autorisé, notamment lorsque le traitement implique la transmission de données sur un réseau, et contre toute autre forme de traitement illicite. Ces mesures doivent assurer un niveau de sécurité adapté aux risques du traitement et à la nature des données à protéger **[34]**.

Le RT doit être en mesure de respecter les exigences de sécurité suivantes **[36]** :

1. Ne collecter que les données nécessaires ;
2. Tenir à jour un inventaire des violations de données à caractère personnel et des mesures prises pour y remédier ;
3. Détruire les informations personnelles identifiables d'une manière sécurisée conformément aux normes et procédures d'élimination des données.

À cet effet, nous proposons dans l'annexe B les mesures correspondant à chaque article de la Loi à prendre en considération dans les traitements.

7 Conclusion

Dans ce troisième chapitre, nous avons développé l'étude conceptuelle de notre application, étape essentielle dans la réalisation des projets informatiques.

Nous avons présenté les différents diagrammes élaborés sur la base de la modélisation UML de notre projet, à savoir : le diagramme de cas d'utilisation (DCU), les diagrammes des activités (DAC) et le diagramme de classe (DCL) ; un rappel des notions de SGBD, de la cryptographie et de la politique de sécurité des

mots de passe s'est avéré nécessaire pour développer et expliquer les choix prônés dans notre projet en matière de gestion et de sécurité des données.

Ainsi, nous ne pouvons clôturer cette phase de conceptualisation sans souligner la nécessité de la mise en œuvre des mesures techniques et organisationnelles pour garantir la sécurité des traitements engagés ainsi que la conformité de ces derniers avec la loi 18-07.

Enfin, ce troisième chapitre constitue une partie essentielle des phases d'élaboration et de conception du processus UP, permettant de préparer le terrain pour la phase de réalisation et de tests abordée dans le chapitre (04) suivant.

Chapitre 4 : Réalisation & implémentation

1 Introduction

Dans ce chapitre, nous présentons la dernière partie de notre projet consacrée à la phase réalisation de l'application ; que nous entamons par la description de l'environnement de développement, suivie par le déroulement des étapes de fonctionnement du système à travers la présentation des différentes interfaces assurant la saisie des données ainsi que le passage d'un module à l'autre.

À la fin de ce chapitre, et pour mieux élucider et démontrer l'implémentation de notre solution, un exemple de jeu de données est déroulé sur le cas de l'ENTP.

2 L'environnement de développement Visual FoxPro

Microsoft Visual FoxPro V.9 est un système de gestion de base de données relationnelle (SGBDR) **[29]** et un environnement de programmation orienté objet conçu pour créer des applications de base de données de bureau. Parmi les caractéristiques du VFP qui nous ont orientés vers ce choix, on peut citer les principales **[34]** :

- **Rapid Application Development (RAD)** : VFP était connu pour ses capacités RAD, permettant aux développeurs de concevoir et de construire rapidement des applications de base de données avec un concepteur de formulaires visuels et un environnement de programmation intuitif.
- **Interactive Development Environment (IDE) :** VFP a un ensemble complet d'outils pour le développement d'applications, notamment un éditeur de code, un concepteur de formulaires, un concepteur de rapports et un débogueur pour le dépannage et le test du code.
- **Table and Database Management** : VFP disposait d'outils intégrés pour créer, gérer et indexer des tables. Il prenait en charge différents types de données et disposait d'un moteur de base de données haute performance.
- **Data Connectivity** : Visual FoxPro prenait en charge diverses sources de données, y compris son format de fichier DBF natif, ainsi que des connexions à des bases de données externes via ODBC (Open Database Connectivity) et d'autres technologies d'accès aux données.

3 Présentation de l'application

Notre application sera présentée à travers le déroulement d'un cas d'étude réel effectué au sein de l'Entreprise Nationale des Travaux aux Puits (E.N.T.P.), des captures d'écran seront affichées au fur et à mesure de l'avancement du déroulement décrivant les fonctions ainsi que l'enchaînement des différentes étapes de l'application.

3.1 Présentation de l'ENTP

L'Entreprise Nationale des Travaux aux puits (E.N.T.P), est une entreprise publique économique basée à Hassi-Messaoud (Ouargla), filiale du groupe Sonatrach activant dans le secteur des hydrocarbures et spécialisée dans le forage et la maintenance des puits, et disposant d'un parc de 72 appareils de forage. Depuis sa création en 1981, elle a réalisé 2900 puits de forage et entretenu 4800 puits à travers tout le territoire national, devenant ainsi un leader incontesté.

L'ENTP est structurée en trois (03) branches d'activité, à savoir, Opérations, Logistique et Administration & Finances, ayant un effectif de 10 000 employés répartis sur plusieurs directions et sites géographiquement distants.

En matière de gestion, l'ENTP dispose d'un système d'information ERP fonctionnel depuis 2010, renforcé par des systèmes et des applications spécialisées couvrant toutes ses activités (ReSHum, BigDOS, GMT).

3.2 Interface d'authentification

Pour accéder à l'application nommée **Conform1807**, l'utilisateur doit s'authentifier par un nom utilisateur et un mot de passe, comme illustré dans la figure 4.1.

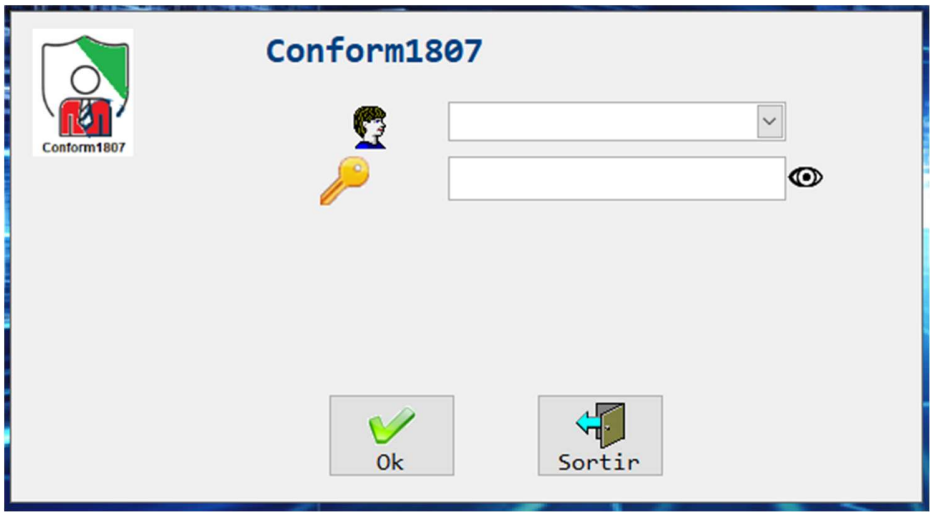


Figure 4.1 : L'interface « Authentification »

Conform1807 est une application de type Desktop sous réseau, constituée de quatre (04) modules de base comme illustré dans la figure 4.2 :

1. Administration de la base de données
2. Gestion des traitements des données à caractère personnel
3. Gestion des demandes de droits des personnes concernées
4. Gestion des violations des données à caractère personnel

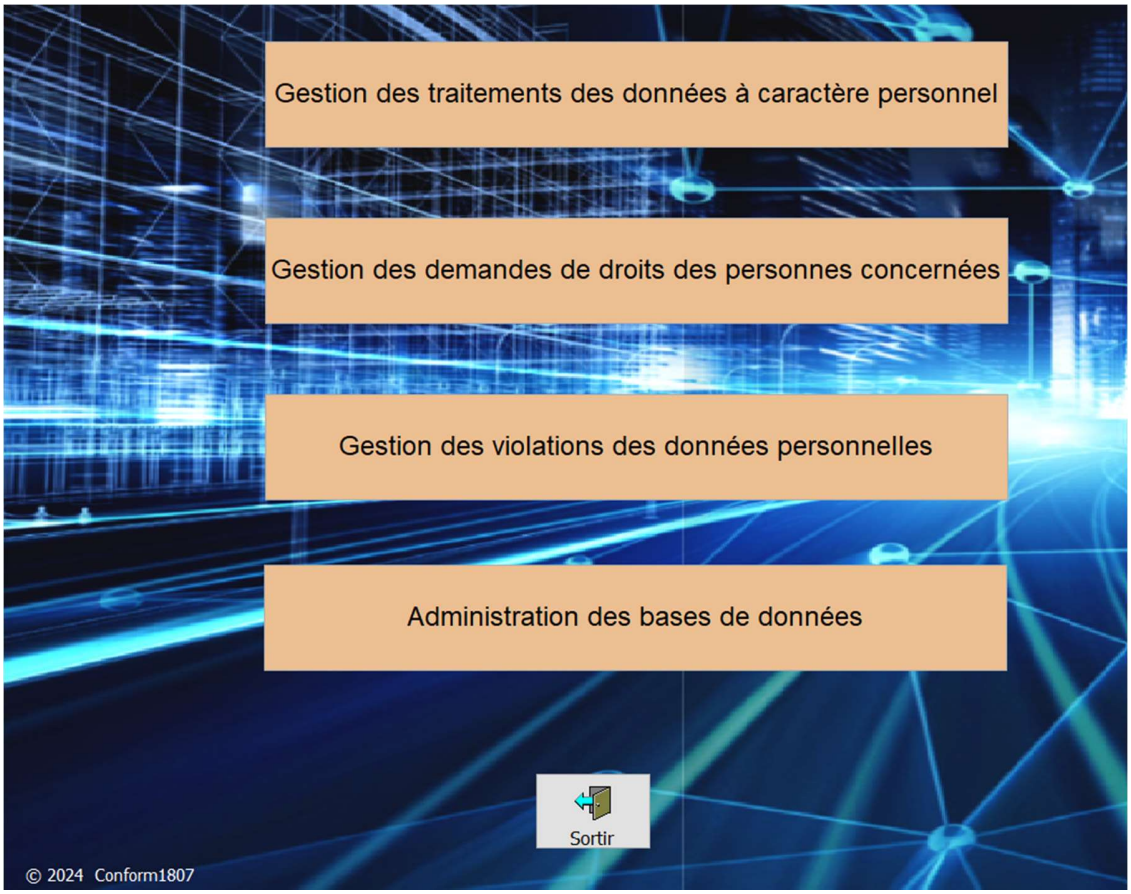


Figure 4.2 : Les modules de l'application *Conform1807*

3.3 Interface du module « Gestion des traitements des DCP »

Afin de dérouler le module de gestion des traitements des DCP, on a préparé un cas réel à appliquer sur les activités du traitement « sélection et recrutement » comme illustré dans la figure 4.3.

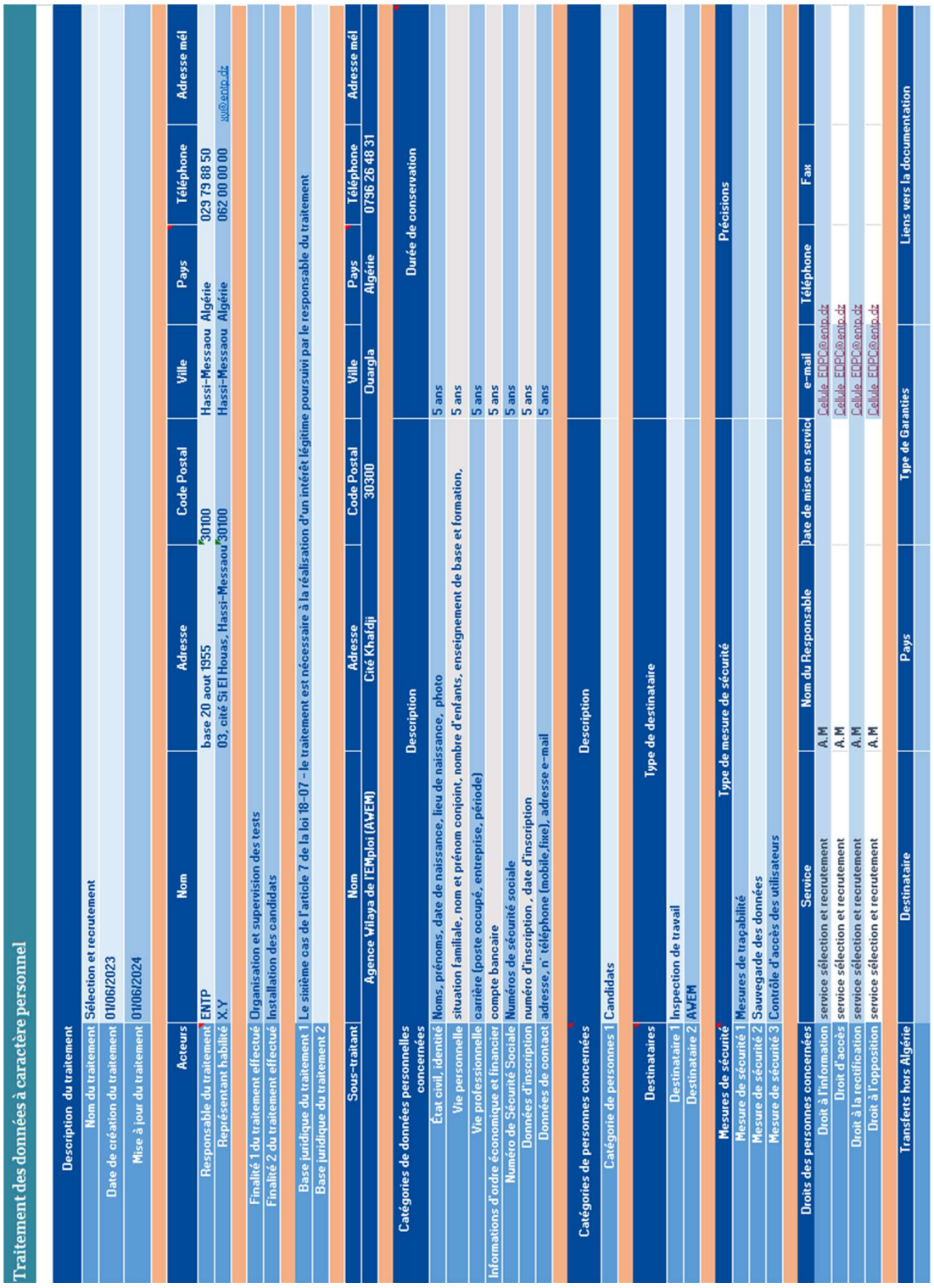


Figure 4.3 : Jeu de données du traitement « sélection et recrutement ».

Le déroulement du jeu de données dans l'application *Conform1807* est schématisé par les figures 4.4, 4.5 et 4.6.

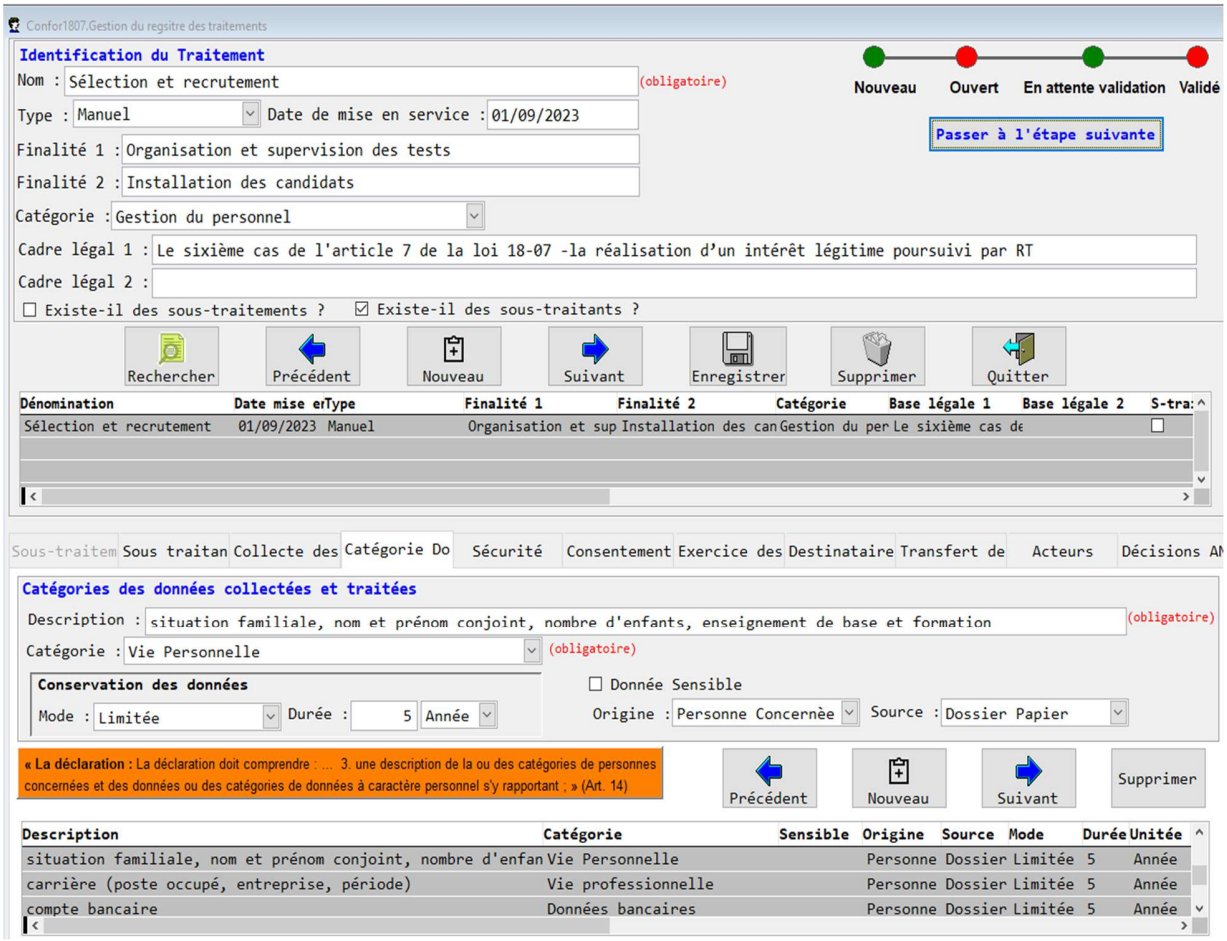


Figure 4.4 : L'interface du module « Gestion des traitements des DCP », avec le volet ''Catégorie des données'' sélectionné

L'enregistrement et la validation des données des sous-traitants du traitement « Sélection & recrutement » est illustré dans la figure 4.5.

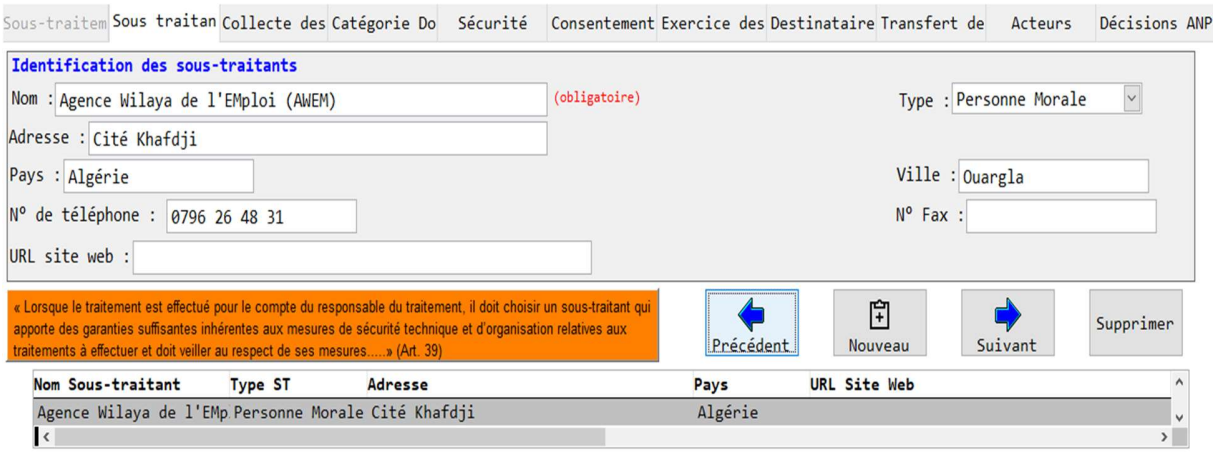


Figure 4.5 : Volet sous-traitant dans le module " Gestion des traitements des DCP »

L'enregistrement et la validation des données de l'exercice des droits des PC du traitement « Sélection & recrutement » est illustré dans la figure 4.6.

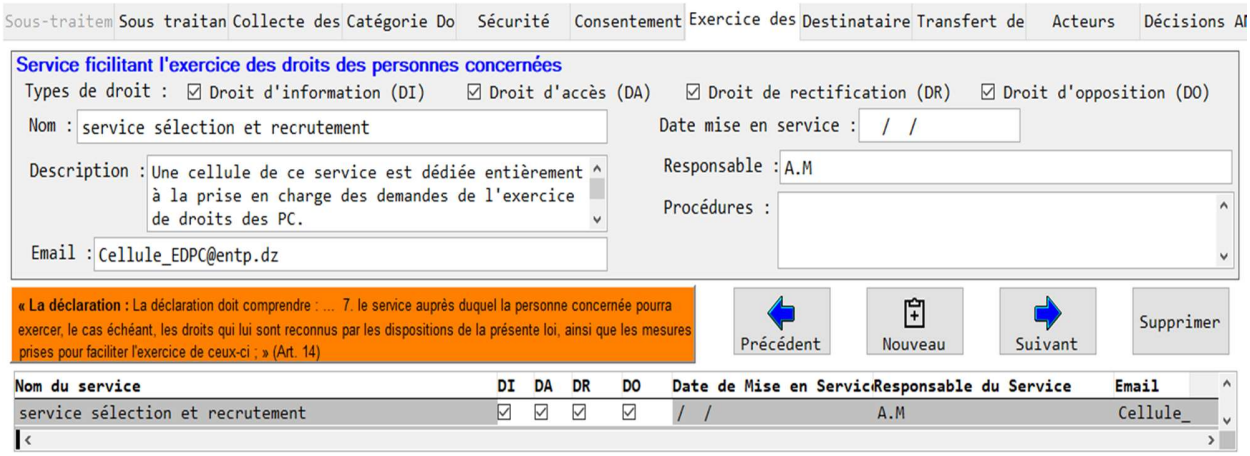
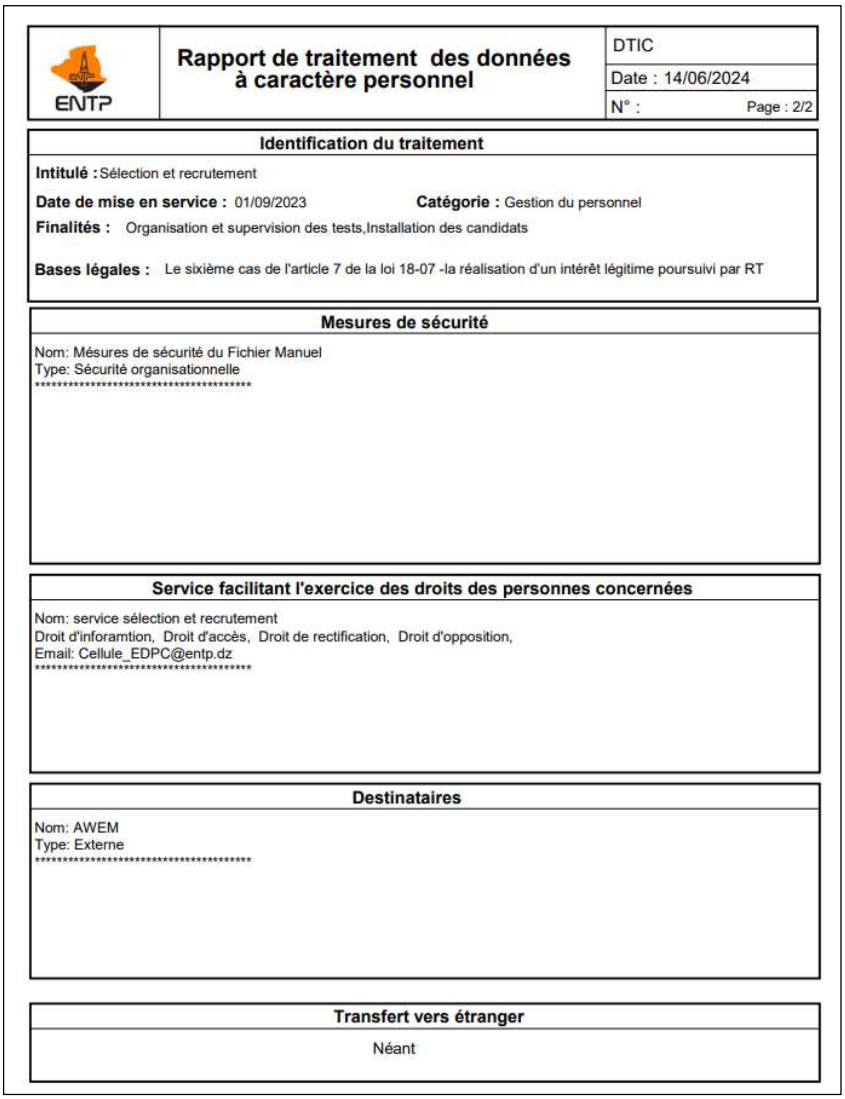


Figure 4.6 : Volet « Exercice des droits » dans le module « Gestion des traitements des DCP »

La première page du rapport de traitement des DCP inclut l'identification du traitement, le RT, RepH, les sous-traitements, les sous-traitants, les catégories des données ainsi que le consentement, comme illustré dans les figures 4.7.

Figure 4.7 : États de sortie « Rapport de traitement des DCP (page 1/2) »

La deuxième page du rapport de traitement des DCP inclut les mesures de sécurité, les services facilitant l'exercice des droits des PC, les destinataires ainsi que les pays de transfert à l'étranger, comme illustré dans les figures 4.8.



ENTP

Rapport de traitement des données à caractère personnel

DTIC
Date : 14/06/2024
N° : Page : 2/2

Identification du traitement

Intitulé : Sélection et recrutement

Date de mise en service : 01/09/2023 **Catégorie :** Gestion du personnel

Finalités : Organisation et supervision des tests,Installation des candidats

Bases légales : Le sixième cas de l'article 7 de la loi 18-07 -la réalisation d'un intérêt légitime poursuivi par RT

Mesures de sécurité

Nom: Mésures de sécurité du Fichier Manuel
Type: Sécurité organisationnelle
****

Service facilitant l'exercice des droits des personnes concernées

Nom: service sélection et recrutement
Droit d'inforamtion, Droit d'accès, Droit de rectification, Droit d'opposition,
Email: Cellule_EDPC@entp.dz
****

Destinataires

Nom: AWEM
Type: Externe
****

Transfert vers étranger

Néant

Figure 4.8 : États de sortie « Rapport de traitement des DCP (page 2/2) »

3.4 Interface du module « Gestion des demandes de droits des PC »

Afin de dérouler le module de gestion des demandes de droits des PC, on a préparé un cas réel du jeu de données de demande d'exercice de droit de la PC illustré dans la figure 4.9.

Demande d'exercice de droit des PC

Demande d'exercice de droit	Titre	Source	Date de la demande	Type de droit demandé			
	Demande de la notation du test de recrutement des opérateurs de mainteanance effectué le 12/09/2023	Demande manuscrite	15/10/2023	Information			

Acteurs	Nom	Adresse	Code Postal	Ville	Pays	Téléphone	Adresse mél
Responsable du traitement	ENTP	base 20 aout 1955	30100	Hassi-Messaou	Algérie	029 79 88 50	
Représentant habilité	X.Y	03, cité Si El Houas, Hassi-Messaoud	30100	Hassi-Messaou	Algérie	062 00 00 00	xy@entp.dz

Personne concernée	Nom prénom	Adresse	Code Postal	Ville	Pays	Téléphone	Adresse mél
	Ali Ben Mohammed	Cité Bamendil,	30300	Ouargla	Algérie		

Catégories de personnes concernées	Description
Catégorie de personnes	Candidats

Données communiquées	Traitement	Réponse	Date de réponse	Finalités	Destinataires	Transferts vers l'étranger	
	Sélection et recrutement	Mr. Ali Ben Mohamed, Test non concluant au concour de recrutement des Opérateurs Maintenance du 12/09/2023 Note globale: 08/20	20/10/2023	Organisation et supervision des tests Installation des candidats	AWEM Ouargla, Inspection de travail Ouargla	-	

	Notification PC	Notification RT		
	20/10/2023	20/10/2023		

Figure 4.9 : Jeu de données de demande d'exercice de droit de la PC

Le déroulement du jeu de données dans l'application *Conform1807* commence par l'introduction de la PC dans le système comme illustré dans la figure 4.10, puis on passera au module « Gestion des demandes de droit des PC comme illustré dans les figures 4.10, la PC doit être préalablement enregistré dans le système, puis on passe au module « Gestion des demandes de droits des PC » pour engager les étapes du traitement de la demande (identification, analyse, traitement, communication et fermeture), comme illustré dans les figures 4.11, 4.12, 4.13 et la dernière figure 4.14 représentant l'état de sortie de la notification à envoyer à la PC pour clôturer le traitement de la demande.

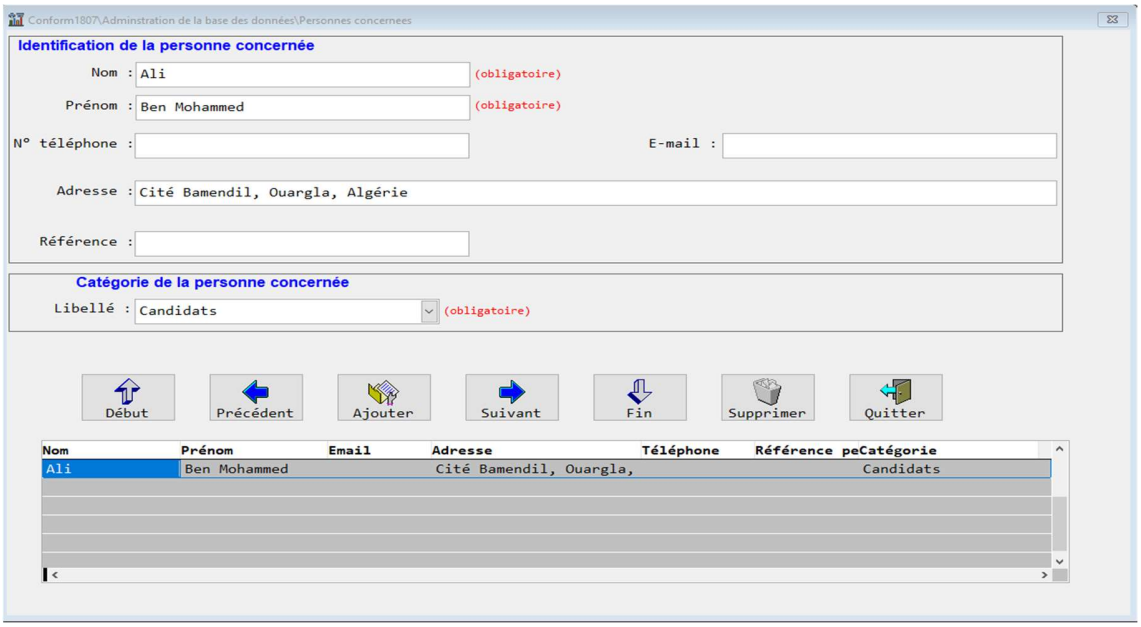


Figure 4.10 : Interface de « M.A.J. des personnes concernées »

La gestion des demandes de droits des PC commence par l'identification de la demande comme illustré dans la figure 4.11.

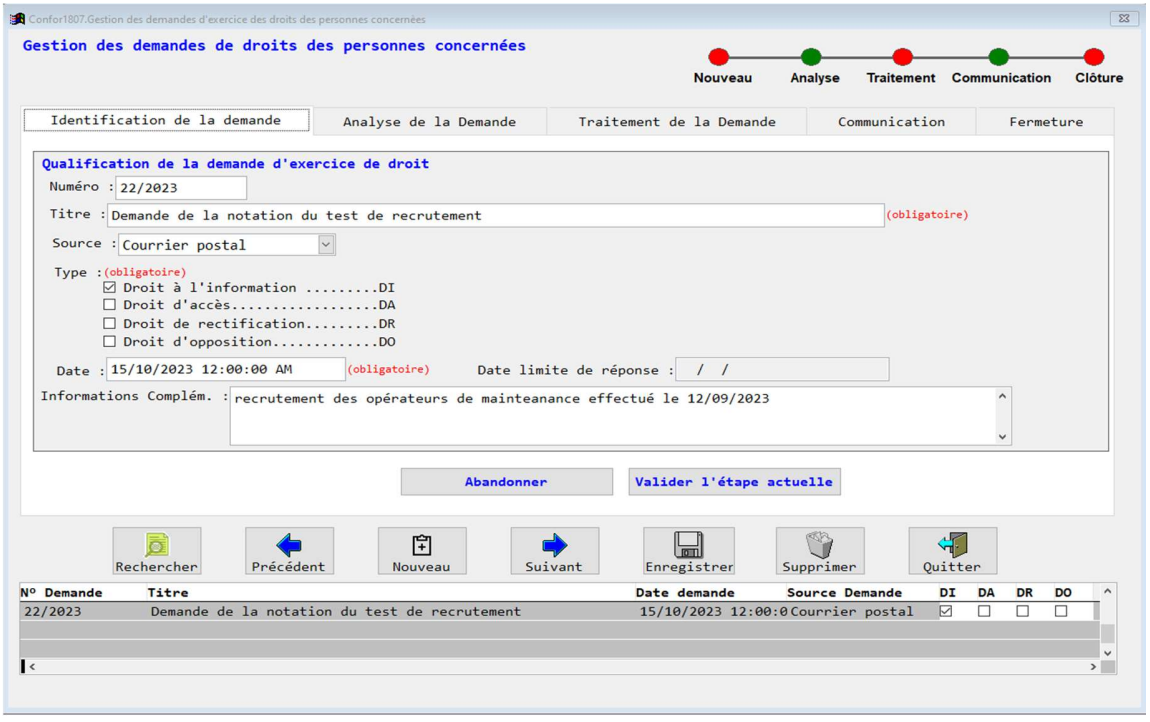


Figure 4.11 : L'interface du module " Gestion des demandes de droits des PC"

Dans l'étape traitement de la demande, on récupère les données du traitement « Sélection & recrutement » pour la traiter, comme illustré dans la figure 4.12.

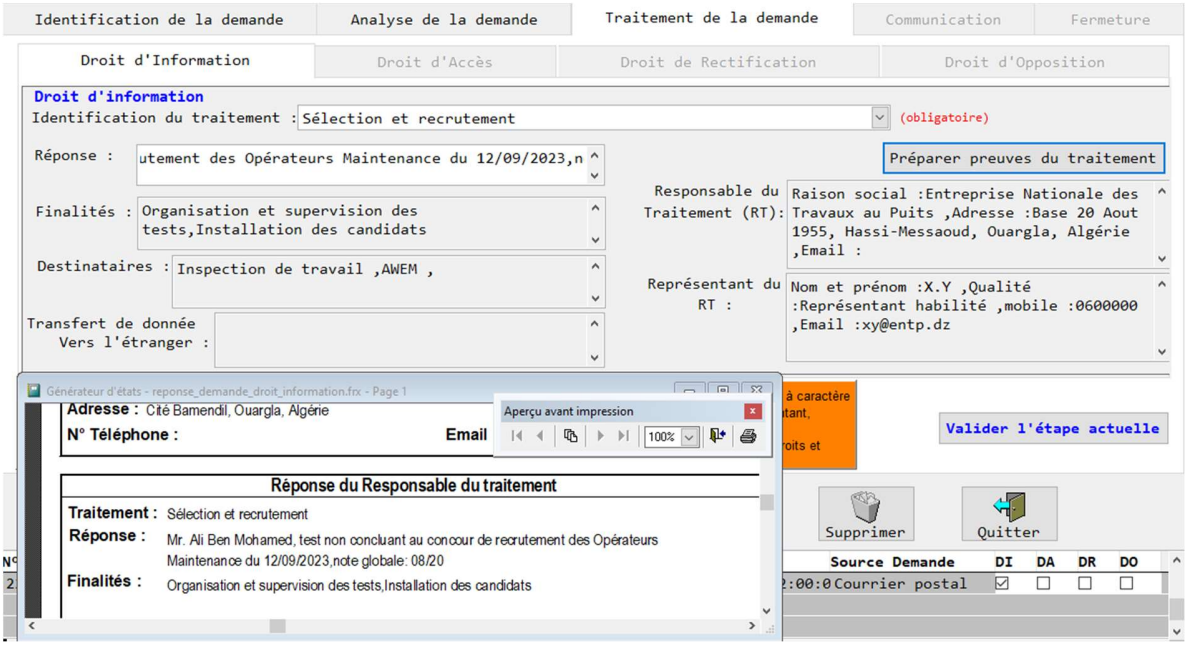


Figure 4.12 : volet « Traitement de la demande » dans le module « Gestion des demandes de droits des PC »

Après l'étape traitement, on passe à l'étape communication où on enregistre la méthode de notification de la PC comme décrit dans la figure 4.13.

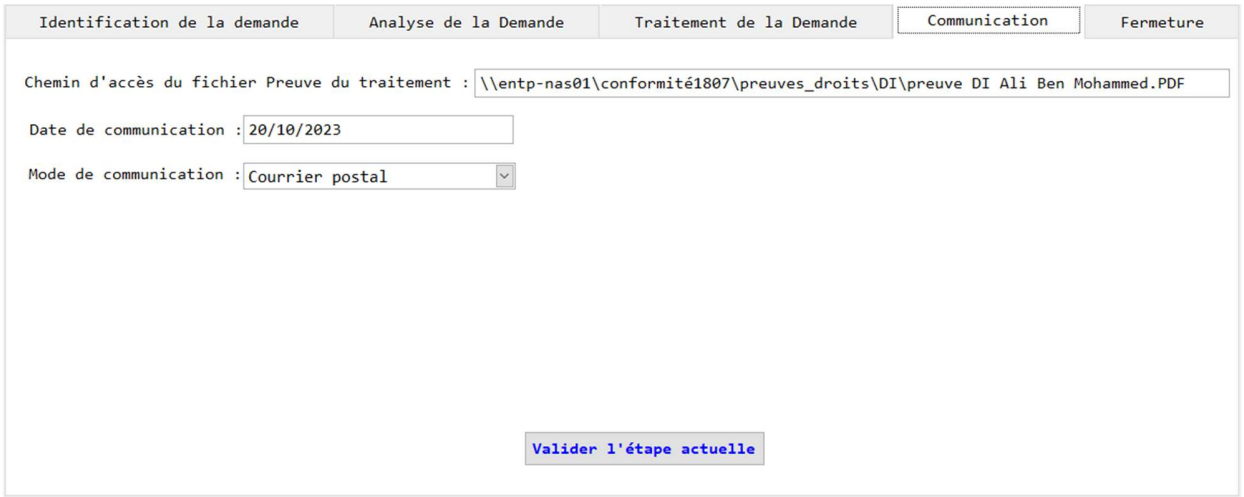
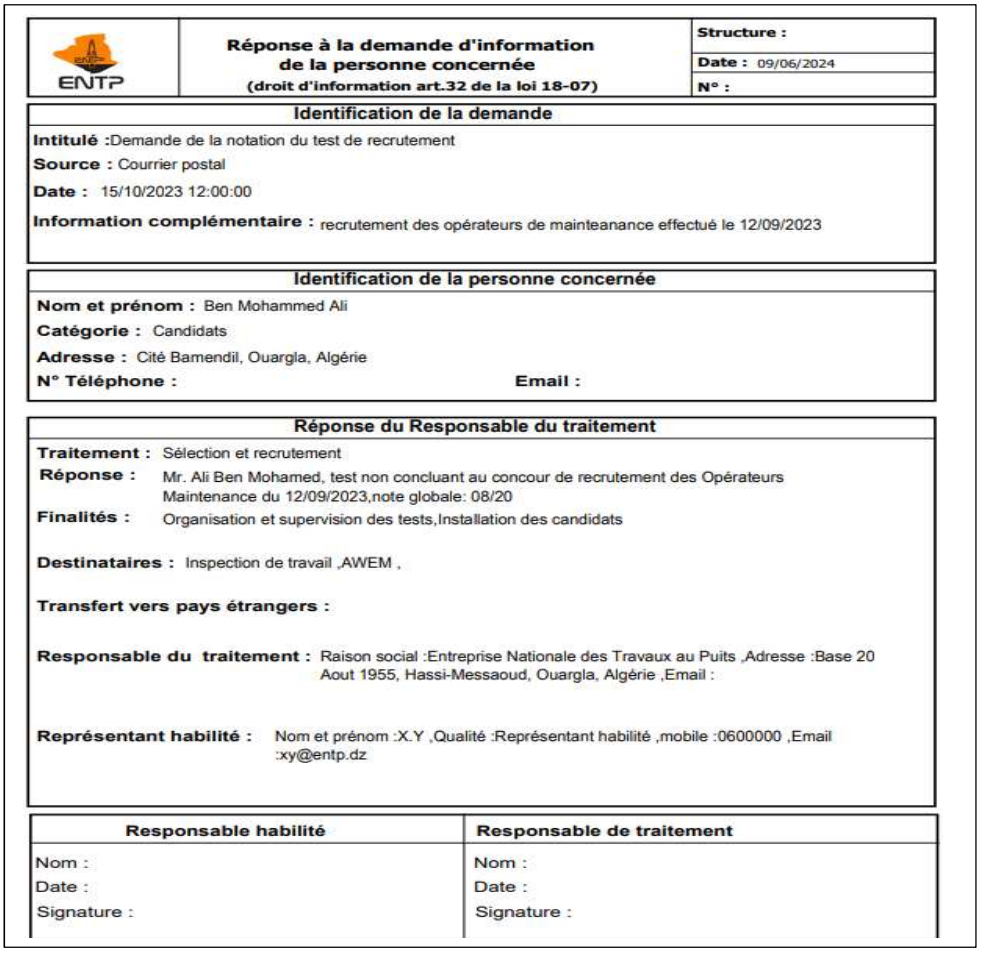


Figure 4.13 : volet « Communication » dans le module « Gestion des demandes de droits des PC »

La présentation de la notification à la PC concernant l'étude de cas est détaillée dans la figure 4.14.



ENTP

Réponse à la demande d'information de la personne concernée
(droit d'information art.32 de la loi 18-07)

Structure :
Date : 09/06/2024
N° :

Identification de la demande

Intitulé : Demande de la notation du test de recrutement
Source : Courrier postal
Date : 15/10/2023 12:00:00
Information complémentaire : recrutement des opérateurs de mainteanance effectué le 12/09/2023

Identification de la personne concernée

Nom et prénom : Ben Mohammed Ali
Catégorie : Candidats
Adresse : Cité Bamendil, Ouargla, Algérie
N° Téléphone : **Email :**

Réponse du Responsable du traitement

Traitement : Sélection et recrutement
Réponse : Mr. Ali Ben Mohamed, test non concluant au concour de recrutement des Opérateurs Maintenance du 12/09/2023,note globale: 08/20
Finalités : Organisation et supervision des tests,Installation des candidats
Destinataires : Inspection de travail ,AWEM ,
Transfert vers pays étrangers :
Responsable du traitement : Raison social :Entreprise Nationale des Travaux au Puits ,Adresse :Base 20 Aout 1955, Hassi-Messaoud, Ouargla, Algérie ,Email :
Représentant habilité : Nom et prénom :X.Y ,Qualité :Représentant habilité ,mobile :0600000 ,Email :xy@entp.dz

Responsable habilité	Responsable de traitement
Nom :	Nom :
Date :	Date :
Signature :	Signature :

Figure 4.14 : États de sortie « Notification à la PC »

3.5 Interface du module « Gestion des violations des DCP »

Pour mettre en œuvre le module de gestion des violations des DCP, nous avons préparé un cas réel basé sur la divulgation de données personnelles d'un candidat à un concours de recrutement sur les réseaux sociaux, comme illustré à la figure 4.15.

Le traitement de ce jeu de données dans l'application Conform1807 permet de suivre les étapes du traitement de la violation des DCP, comme montré aux figures 4.16 et 4.17. La dernière figure 4.18 présente l'état final de la notification de la violation des DCP, à envoyer à l'ANPP et à la PC.

Violation des données à caractère personnel

	Intitulé	Type	Date de detection	Description
Identification de la violation	Dévulgation des données personnelles du candidat au recrutement	Atteinte à la confidentialité	01/05/2024	Rapport du violation recu du RSSI le 10/05/2024 concernant la divulgation aux tiers à travers les réseaux sociaux (forum de discussion), des DCP (note, adresse, n° téléphone) du candidat Ali Ben Mohammed objet du traitement sélection & recrutement.

	Impacts Probables de cette Violation	Nature de la Violation	Personnes concernées affectées	Données sensibles
Analyse de la violation	Perte de confidentialité des DCP	- Documents perdu - Divulgation non autorisé - Accès non autorisé	Candidats	Non

	Description du traitement	Mesures immédiates de limitation des effets négatifs de la violation de données
Traitement de la violation	- Contacter la plateforme de réseau social pour demander la suppression immédiate des données divulguée - Informer rapidement les individus concernés par la divulgation, - Déterminer comment la divulgation s'est produite et identifier les responsables - Prendre les mésures correctives et préventives, - Lancer une campagne de sensibilisation en interne.	

Notification	RT	PC	ANPDP	
Date	03/05/2024	03/05/2024	03/05/2024	

Figure 4.15 : Jeu de données de violation des DCP.

Le RSSI enregistre le traitement des violations des DCP dans l'application, conformément à ce qui est expliqué dans la figure 4.16.

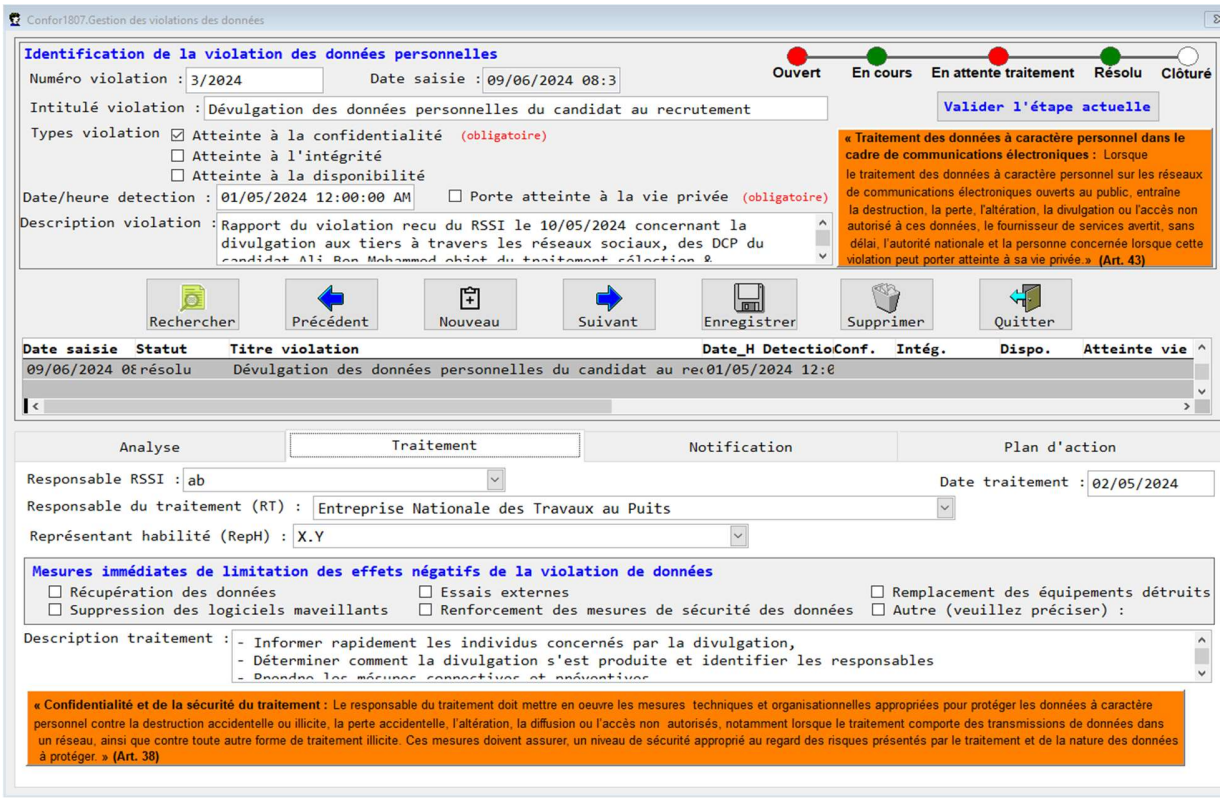


Figure 4.16 : L'interface du module « Gestion des violations des DCP » avec le volet ''Traitement'' sélectionné.

Après la phase de traitement, la notification des parties prenantes est effectuée dans l'application, tel que décrit dans la figure 4.17.

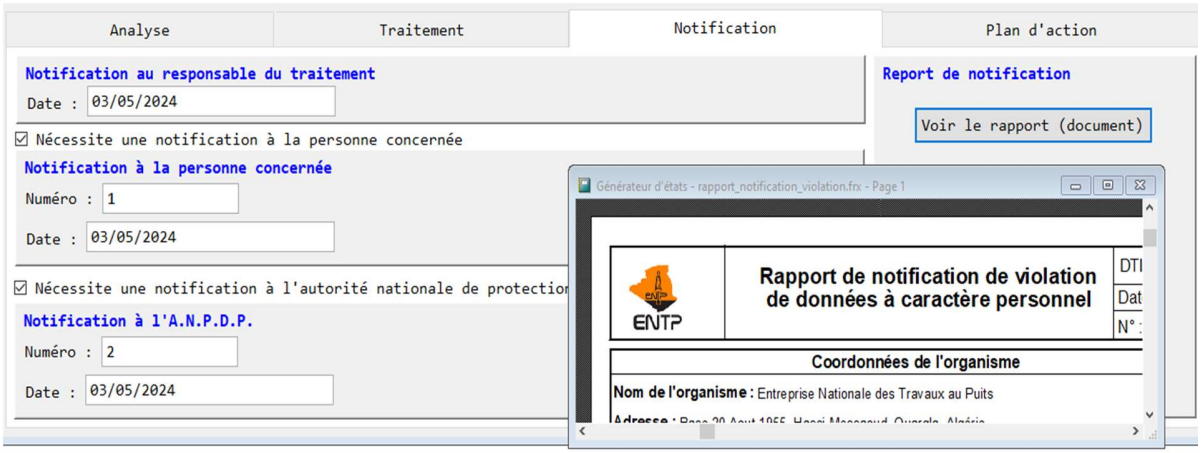


Figure 4.17 : Volet « Notification » dans le module « Gestion des violations des DCP »

Le rapport de notification de la violation des DCP pour l'étude de cas est détaillé dans la figure 4.18.

Figure 4.18 : État de sortie « Rapport de notification de violation de DCP »

3.6 Interface de gestion des utilisateurs

L'interface « Rôles » mis en œuvre, comme illustré dans la figure 4.19 pour configurer les autorisations d'accès au système, ainsi de protéger le système.

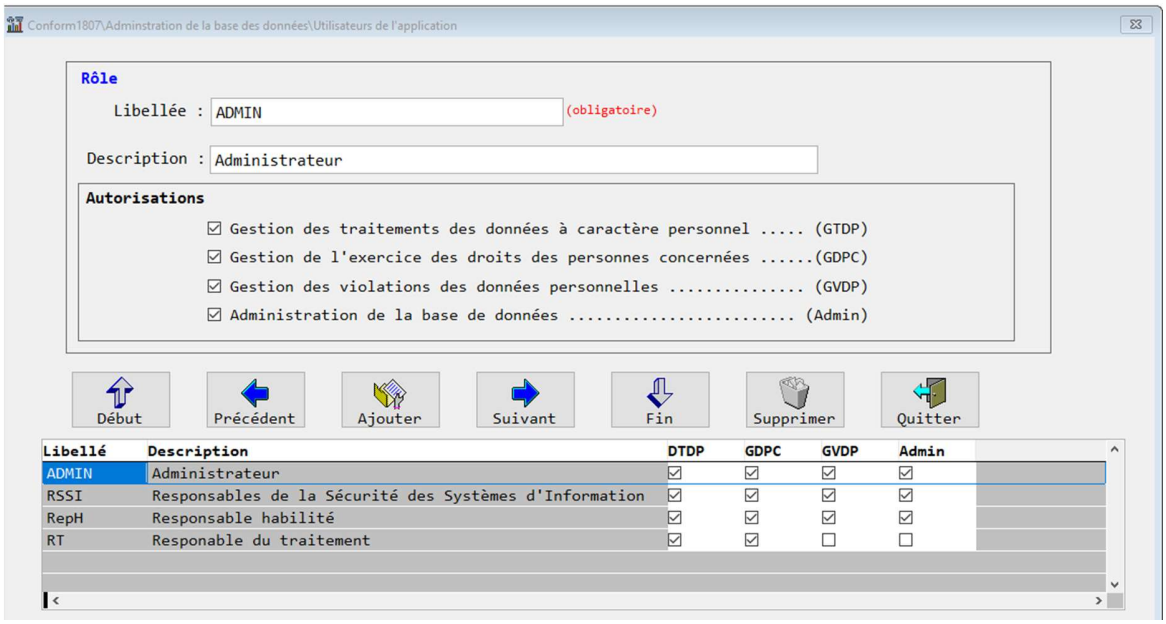


Figure 4.19 : L'interface « Rôles »

Afin de permettre de gérer les utilisateurs, l'interface « Gestion des utilisateurs » est mis en œuvre, comme illustré dans la figure 4.20.

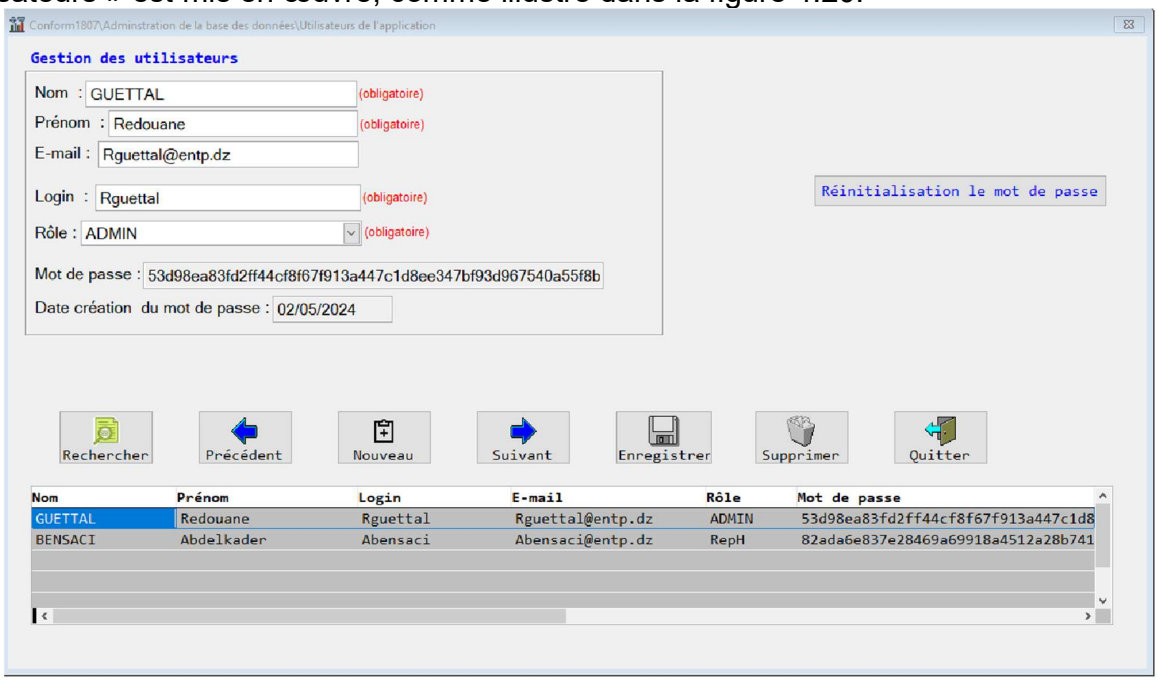


Figure 4.20 : L'interface « Gestion des utilisateurs ».

4 Conclusion

Dans ce quatrième et dernier chapitre de notre thèse, nous avons décrit la phase de réalisation de l'application, en adoptant une approche fonctionnelle basée dur l'implémentation et l'itération des jeux de tests pour ajuster et améliorer le système telle que stipule la méthodologie UP.

A cet effet, des cas d'études ciblés et adaptés à chaque module ont été choisis et déroulés selon plusieurs scénarios dans l'application Conform1807 pour vérifier et mettre en œuvre toutes les fonctionnalités de cette dernière; les résultats obtenus ont été satisfaisants et ont contribué à raffiner notre solution pour aboutir la version finale présenté dans ce chapitre.

Conclusion générale

La protection des données à caractère personnel est devenue un enjeu majeur dans un monde de plus en plus digitalisé, où la circulation rapide des informations et l'omniprésence des technologies posent des défis considérables en matière de sécurité et de confidentialité. Dans ce contexte, notre étude s'est focalisée sur le développement d'une application informatique dédiée à la mise en conformité avec la loi 18-07, promulguée en 2018 en Algérie et entrée en application à partir du 10 aout 2023.

Notre application se distingue par sa capacité à fournir aux entreprises un outil efficace pour se conformer aux exigences de la Loi 18-07 ; elle intègre les principes de la protection des données à caractère personnel comme les droits des personnes, la notification des violations des données personnelles à titre d'exemple, et non de manière exhaustive. En offrant une interface conviviale, des évaluations de conformité automatisées et des conseils personnalisés, elle répond à un besoin critique sur le marché local.

La loi 18-07 représente une avancée significative dans le cadre juridique de la protection des données à caractère personnel en Algérie, visant à réguler de manière stricte le traitement de ces données, depuis leur collecte jusqu'à leur diffusion. Cependant, la mise en conformité avec cette législation soulève des défis techniques et organisationnels notables, ainsi que des risques de non-conformité, tels que des sanctions légales et des atteintes à la réputation des entités concernées. Notre application répond à ces défis en facilitant la gestion des traitements de données, le respect des droits des personnes concernées et la gestion des violations de données, contribuant ainsi à une meilleure conformité avec les exigences légales.

En Algérie, il n'existait jusqu'à présent aucune application spécifiquement dédiée à la mise en conformité avec la loi 18-07. Les solutions internationales disponibles sont souvent onéreuses, complexes à implémenter, et ne tiennent pas compte des spécificités de la législation algérienne. Notre travail comble cette lacune en proposant une solution locale, accessible et parfaitement adaptée aux besoins spécifiques des entreprises algériennes.

Ce mémoire apporte une contribution significative à la protection des données à caractère personnel en Algérie. L'application développée constitue un outil précieux pour les entreprises, leur permettant de se conformer efficacement à la loi 18-07 et de renforcer la confiance des consommateurs. Les résultats obtenus montrent que notre approche est à la fois pratique et innovante, ouvrant la voie à de futures recherches et développements pour améliorer encore la gestion et la protection des données personnelles dans le contexte algérien.

.

En guise de perspective, une extension de ce travail est envisagée par la migration de notre application vers une solution web, utilisant SQL comme

système de gestion de base de données. Cette migration permettra d'améliorer l'accessibilité et la flexibilité de l'application, facilitant son utilisation sur diverses plateformes et par différents utilisateurs. De plus, l'adoption de SQL offrira des capacités robustes de gestion des données, renforçant ainsi la performance et la sécurité du système.

L'ajout du module de gestion des consentements est crucial pour se conformer aux exigences légales de collecte et d'utilisation des données personnelles. Un module dédié à cette fonction permettra aux entreprises de suivre et de documenter les consentements des individus de manière efficace. Cette fonctionnalité assurera que les entreprises obtiennent, stockent et gèrent les consentements de manière conforme et transparente, renforçant ainsi la protection des droits des personnes concernées.

Enfin, la gestion des audits est un aspect fondamental pour maintenir et prouver la conformité continue avec la loi 18-07. Un module d'audit intégré permettra de planifier, exécuter et documenter les audits internes et externes. Cette fonctionnalité fournira aux entreprises des outils pour évaluer leur conformité, identifier les faiblesses et mettre en œuvre des mesures correctives en temps opportun, assurant ainsi une amélioration continue de leurs pratiques de gestion des données. Ces perspectives d'évolution enrichiront notre application, la rendant encore plus complète et efficace dans le soutien des entreprises algériennes pour une conformité rigoureuse et continue avec la loi 18-07.

Bibliographies

[1] Alain F. Westin: Privacy and Freedom, USA, 1967.

[2] Sara Baase, A Gift of Fire: Social, Legal, and Ethical Issues for Computing Technology.

[3] Ibrahim Coulibaly, thèse de doctorat de l'université de Grenoble, thème : La protection des données à caractère personnel dans le domaine de la recherche scientifique, 2011.

[4] CNIL, URL : ttps://www.cnil.fr (consulté le 01/04/2024).

[5] le Groupe d'experts sur les données sensibles (GEDS) du réseau Portage au nom de l'Association des bibliothèques de recherche du Canada (ABRC), « Boîte à outils pour les données sensibles — destinée aux chercheurs», URL : ttps://www.carl-abrc.ca, Septembre 2020.

[6] ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification, European Data Protection Law Review (EDPL), 2020 (consulté le 05/04/2024).

[7] Data Protection Africa, URL : https://www.dataprotection.africa, (consulté le 13/04/2024).

[8] Constitution algérienne (2020), JORA n° 82 du 30/12/2020.

[9] Loi n° 09-04 du 5 aout 2009, JORA n° 47 du 16/08/2009.

[10] Loi n° 18-04 du 10 mai 2018, JORA n° 27 du 13/05/2018.

[11] L'Autorité nationale de protection des données à caractère personnel (ANPDP), URL : https://www.anpdp.dz, (consulté le 07/04/2024).

[12] Décret présidentiel n° 20-05 du 20 janvier 2020, JORA n° 4 du 26/01/2020

[13] Rossi J., revu Geopolitics of Risk Working Papers, thème : Qu'est-ce que le droit à la protection des données à caractère personnel?, 2018.

[14] Guillaume Piolle, thèse de doctorat de l'université de Joseph Fourier 1-Grenoble, thème : Agents utilisateurs pour la protection des données personnelles : modélisation logique et outils informatiques, 2009.

[15] Thiago Moreira da Costa, thèse de doctorat de l'université de Grenoble Alpes sur le thème : OPP_IoT An ontology-based privacy preservation approach for the Internet of Things, 2017.

[16 Karina SOKOLOVA PEREZ, thèse de doctorat de l'université de technologie de Troyes, thème : Bridging the Gap between Privacy by Design and Mobile Systems by Patterns, 2016.

[17] George Danezis et al., Privacy and Data Protection by Design - from policy to engineering, 2014, (European Union Agency for Network and Information Security, enisa, URL : www.enisa.europa.eu), page : 3.

[18] Gilles W. van Blarkom, John J. Borking, and Eddy Olk, Handbook of Privacy and Privacy-Enhancing Technologies - *The case of Intelligent Software Agents*, The Hague, The Netherlands, 2003, (pages 33–54).

[19] La norme ISO/IEC29134 fournit des lignes directrices sur la manière de réaliser PIA (privacy impact assessment) et sur la manière de structurer les rapports de PIA, URL : https://www.iso.org.

[20] AEPD (Agencia Española de Protección de Datos – Autorité espagnole de protection des données), Guidelines Personal Data Breach Notification, 2018.

[21] David McCandless, World's Biggest Data Breaches & Hacks. https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ (consulté le 12/04/2024).

[22] Loi n° 18-07 du 10 juin 2018, JORA n° 34 du 10/06/2018.

[23] Décret présidentiel n° 22-187 du 18 mai 2022, JORA n 35 du 24/05/2022.

[24] Philippe Rigaux, Cours de bases de données, 2001.

[25] Alexandre Feugas, thèse de doctorat de l'université de Lille 1 Sciences et Technologies, thème : Une Approche Agile, Fiable et Minimale pour le maintien de la qualité de service lors de l'évolution d'applications à base de processus métiers, 2014.

[26] I. Wautelet et al. , le nified Process comme méthodologie de gestion de projet informatique, IAG Working Papers, 2004

[27] Joseph GABAY et al. UML 2 Analyse et conception, mise en œuvre guidé avec étude de cas, Dunos, Paris, 2008.

[28] Olivier Capuozzo., Cas d'utilisation, une introduction, Éditions CERTA (2004).

[29] Azhar Susanto, Database Management System, International Journal of Scientific & Technology Research, volume 8, URL: https://www.ijstr.org, 2019.

[30] Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, 2020.

[31] Jérémy Jean, Thèse de doctorat de l'université Paris Diderot sur le thème : Cryptanalyse de primitives symétriques basées sur le chiffrement AES, 2013

[32] Mathieu VALOIS, Thèse de doctorat de l'université sur le thème : Mesure de la robustesse des mots de passe, 2019

[33] Recommandations relatives à l'authentification multifacteur et aux mots de passe, ANSSI-PG-078, 2021.

[34] Sihem Hassani, Alegria - Data Protection Overview, URL : https://www.dataguidance.com/notes/algeria-data-protection-overview, (consulté le 17/04/2024).

[35] Inter Soft Associates, Les fonctionnalités techniques avancées de Visual FoxPro comprenaient le traitement complexe des données, URL: https://intersoftassociates.com/.

[36] Référentiel National de Sécurité de l'Information, Ministère de la Poste et des Télécommunications (MPT), URL : https://www.mpt.gov.dz, 2020.

[37] Le décret exécutif n° 98-257 du 25 aout 1998, JORA n° 63 du 26/08/1998

[38] Zina YACOUB, De la protection des données personnelles à la lumière de la loi n° 18-07 : une nouvelle responsabilisation pour les entreprises, Revue Académique de la Recherche Juridique (RARJ), 2021.

[39] Pascal Roques et Franck Vallée, UML 2 en action : de l'analyse des besoins à la conception, Eyrolles - Paris, 2007.

[40] Besoins fonctionnels & Besoins non fonctionnels -, URL : https://savoir.plus/besoins-fonctionnels-non-fonctionnels/ (visité le 16/05/2024).

[42] Christian Soutou et Frédéric Brouard. UML 2 pour les bases de données, Éditions Eyrolles, 2012.

[43] Stéphane Crozat, Introduction au passage UML-Relationnel : classes et associations, 2018.

[44] UML SysML, URL : https://www.uml-sysml.org (consulté le 28/05/2024).

[45] Jaap-Henk Hoepman, Privacy Design Strategies, 2013, URL: https://arxiv.org/abs/1210.6621v2

Annexe A : Exemples sur les violations des DCP

Entité	Période	Description
France Travail	Mars 2024	La fuite de données de 43 millions de personnes suite à une cyberattaque. Les données compromises incluent des noms, des dates de naissance, des adresses postales, des numéros de téléphone, des adresses e-mail, des identifiants France Travail et des numéros de sécurité sociale (pour certains) [4].
LastPass	2022	33 millions d'enregistrements du géant gestionnaire de mots de passe LastPass ont été perdus.
AT&T	2021	La fuite de données a touché 7,6 millions d'utilisateurs actuels d'AT&T, 65,4 millions d'anciens abonnés. Les informations exposées comprenaient des données sensibles telles que les noms, les adresses e-mail, les numéros de téléphone et les numéros de sécurité sociale.
Programme d'assurance maladie indonésien (BPJS Kesehatan)	Mai 2020	Les données personnelles sensibles de plus de 279 millions d'enregistrements d'Indonésiens auraient été divulguées, qui comprennent les cartes d'identité nationales, les informations d'enregistrement fiscal et les numéros de téléphone portable.
Firebase	2018	100 millions d'enregistrements de données d'utilisateurs ont été volés. Les informations divulguées comprenaient des mots de passe et des identifiants d'utilisateurs, des enregistrements de localisation GPS, des données financières, des messages de *chat.*
Facebook	Avril 2021	533 millions d'enregistrements ont été perdus. Les informations divulguées comprenaient noms complets, emplacements, renseignements biographiques.
	2018	Avec 10 millions de dossiers perdus, Cambridge Analytica, dirigée à l'époque par Steve Bannan, a recueilli des profils au début de 2014 pour construire un système qui pourrait profiler les électeurs américains et les cibler avec des annonces politiques.

Annexe B : Mesures techniques et organisationnelles

Articles	Mesures
9	Il faut s'assurer que l'organisme a mis en œuvre les mesures suivantes : • Évaluer les activités de traitement (y compris les registres de traitement des données) de l'organisme, • Revoir les lois applicables pour s'assurer que les données sont traitées de façon licite, • Veiller à ce que les données soient validées pour garantir leur exactitude, • Revoir la politique de conservation des données et les procédures de destruction des données, • Revoir les processus afin de garantir l'intégrité et la confidentialité des données.
12	Il faut s'assurer que l'organisme : • À identifier tous les traitements des données à caractère personnel, • À mettre en œuvre des mécanismes pour faire la déclaration de ces traitements auprès de l'autorité nationale, • À mis en place un registre de traitement.
13 et 14	L'application *Conform1807* intègre les dispositions des articles 13 et 14, assurant ainsi la conformité avec ses exigences.
16	Il faut s'assurer que l'organisme : • À identifier les registres (exemple : registre de doléances) ouverts au public, • Mettre en place une procédure de gestion et de déclaration de ce type de registre, • Mettre en place une procédure d'information des personnes concernées qui en font la demande.
32, 34, 35 et 36	L'application *Conform1807* intègre cet article en prenant en charge des mesures techniques et en mettant en place une politique de gestion des droits des personnes concernées, basée sur des mesures organisationnelles.
38	Il faut s'assurer que l'organisme : • À rédiger, valider (par la DG) et communiquer aux parties prenantes une politique de sécurité de l'information, • À mettre en place un processus de gestion et d'appréciation des risques, • A un plan de traitement des risques,

	• Sur la base du plan de traitement des risques, met en œuvre des mesures techniques et organisationnelles pour sécuriser, contrôler et gérer les données à caractère personnel qu'elle traite, • À établir des procédures qui fournissent des instructions sur la manière de traiter les données à caractère personnel sans enfreindre la loi et d'autres exigences légales. • À déterminer si les personnes autorisées à traiter les données suivent les instructions du responsable du traitement, • À mettre en place des mesures en cas de non suivi des instructions du responsable du traitement.
43	Il est essentiel de s'assurer que l'organisme a mis en place un processus de gestion des incidents, comprenant l'identification des systèmes concernés, des incidents redoutés et du processus de gestion des incidents, ainsi que l'identification des contours d'une déclaration à l'ANPDP et l'inventaire des incidents de violations de données, ces deux derniers points étant assurés par l'application Conform1807.
44	Il est nécessaire de s'assurer que l'organisme a documenté le traitement de la manière suivante : un processus formalisé, des données cartographiées, des données classifiées, et un registre des traitements documentés, ce dernier point étant assuré par l'application Conform1807.