Délibération n° D-188-2020 en date du 14/12/2020 régissant l'Analyse d'impact relative à la protection des données (AIPD)

La CNDP (Commission Nationale de contrôle de la protection des Données à caractère Personnel),

Sous la présidence de Monsieur Omar Seghrouchni ;

Prenant en considération les observations des membres Madame Souad El Kohen, Messieurs Driss Belmahi, Abdelaziz Benzakour, Brahim Bouabid ;

Vu l'article 24 de la Constitution du Royaume qui dispose que : « Toute personne a droit à la protection de sa vie privée » ;

Vu la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel à laquelle le Royaume du Maroc a adhéré en date du 28/05/2019 ;

Vu la loi n° 09-08 promulguée par le Dahir 1-09-15, du 18 février 2009, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (B.O. n°5714 du 05/03/2009) ;

Vu le règlement intérieur de la CNDP (approuvé par décision du Premier Ministre n° 3-33-11 du 28 mars 2011 / B.O. n° 5932 du 07/04/2011) ;

Vu les observations de Madame Souad El Kohen, Messieurs Driss Belmahi, Abdelaziz Benzakour et Brahim Bouabid, rapporteurs désignés par la Commission.

La CNDP rappelle qu'en vertu des dispositions des articles 23 et suivants de la loi 09-08, cette délibération édicte les principes à respecter pour l'évaluation des risques attentatoires à la vie privée et à la protection des données à caractère personnel susceptibles d'avoir lieu suite à un traitement donné.

Tenant compte du cadre légal international et des bonnes pratiques régissant les analyses d'impact relatives à la protection des données, la CNDP entend promouvoir le principe de responsabilisation des entités concernées, afin de les accompagner dans leur démarche d'identification et d'évaluation des situations susceptibles de présenter le plus de risques pour les droits et libertés des personnes concernées.

Pour ce faire, la CNDP adopte les principes et lignes directrices suivantes :

Définitions

- Par **analyse d'impact** relative à la protection des données, désignée ci-après par analyse d'impact, la CNDP entend un processus dont l'objet est de décrire un traitement, d'en évaluer la nécessité ainsi que la proportionnalité et d'aider à la

gestion des risques pour les droits et libertés des personnes physiques liés au traitement de leurs données à caractère personnel, en les évaluant et en déterminant les mesures nécessaires pour y faire face.

Il s'agit d'un outil important au regard du principe de responsabilité, compte tenu de son utilité pour les responsables de traitement, non seulement aux fins de mise en œuvre de traitements de données respectueux de la vie privée, mais également pour asseoir leur capacité à démontrer que des mesures appropriées ont été prises pour assurer leur conformité à loi ; à savoir la minimisation des données collectées, l'obligation de sécurisation de ces dernières, le respect du Privacy by design et Privacy by default.

- Un **risque** sur la vie privée est une situation qui décrit un événement redouté (atteinte à la confidentialité, la disponibilité ou l'intégrité des données, et ses impacts potentiels sur les droits et libertés des personnes) et ses effets (toutes les menaces qui permettraient qu'il survient), estimés en termes de gravité (pour les personnes concernées) et de probabilité.

- La **gestion du risque** peut, quant à elle, être définie comme un ensemble d'activités coordonnées dans le but de diriger et de piloter un organisme vis-à-vis du risque.

- La **proportionnalité** du traitement des données, s'entend de sa pertinence au regard de la finalité légitime poursuivie, et de sa limitation à ce qui est nécessaire au regard des intérêts, droits et libertés des personnes concernées ou de l'intérêt public. Il ne doit pas induire une ingérence disproportionnée dans ces intérêts, droits et libertés. Le principe de proportionnalité doit être respecté à toutes les étapes du traitement, y compris au stade initial, c'est-à-dire lorsqu'il est décidé de procéder ou non au traitement des données.

Contexte d'utilisation

L'Analyse d'Impact relative à la Protection des Données (AIPD) est utilisée dans différents contextes par d'autres réglementations. Elle est utilisée, en particulier, pour matérialiser les responsabilités dans le contexte des réglementations qui s'appuient sur le principe d' « accountability » ou de responsabilisation. En l'espèce, l'Analyse d'Impact relative à la Protection des Données (AIPD) est établie par le Responsable de Traitement qui doit la présenter, en cas de contrôle, à l'autorité en charge de la protection des données à caractère personnel. Dans le cas de traitements sensibles dont la liste est précisée par l'autorité de

contrôle, l'Analyse d'Impact relative à la Protection des Données (AIPD) est présentée pour validation, préalablement à tout déploiement de ces traitements.

La réglementation au Maroc s'appuie sur le régime de la déclaration et pourrait évoluer vers celui de la responsabilisation « accountability » réputée comme étant plus souple et mieux alignée sur les besoins de l'écosystème numérique. Cependant, cette évolution doit être préparée, structurée et fondée sur des principes clairs et sur une mise en œuvre efficace et transparente, par les Responsables de Traitement. La CNDP (Commission Nationale de contrôle de la protection des Données à caractère Personnel) s'inscrit dans cette logique de simplification afin de favoriser l'accompagnement des Responsables de Traitement dans le déploiement de cette culture de responsabilisation et de contrôle a posteriori.

L'étude d'Analyse d'Impact relative à la Protection des Données (AIPD) est un outil d'Analyse des Risques sur la Vie Privée. Le principe de proportionnalité y est décliné selon les contextes opérationnels et les exigences de respect de la vie privée, approuvés par l'Autorité de Contrôle, le risque zéro n'existant pas.

Ainsi, en prévision de potentielles évolutions réglementaires, la CNDP (Commission Nationale de contrôle de la protection des Données à caractère Personnel) souhaite promouvoir le principe des analyses de risques dans le domaine de la protection de la vie privée.

Pour ce faire, la Commission encourage :

- Les sous-traitants à formaliser des Analyses d'Impact relative à la Protection des Données (AIPD) afin de simplifier les dossiers de conformité à la loi 09-08 de leurs clients. Ces AIPD seraient référencées auprès de la Commission, sans être considérées comme constituant une quelconque autorisation de mise en œuvre puisque le client final, reste à ce stade, entièrement responsable de l'intégration du dispositif du sous-traitant dans son écosystème. Cette disposition optimisera et favorisera la normalisation de l'instruction des dossiers de notification en facilitant l'étude des caractéristiques des traitements gérés par les sous-traitants.
- Les Responsables de traitement à mettre en place des Analyses d'Impact relative à la Protection des Données (AIPD), dans le cas des traitements définis ci-après, en vue de mieux expliquer les mesures prises pour la protection des données à caractère personnel aux personnes concernées et aussi en vue de faciliter leurs échanges avec la CNDP (Commission Nationale de contrôle de la protection des Données à caractère Personnel).

Traitements concernés

La CNDP établit les listes des traitements concernés et non concernés par cette délibération. Ces listes sont évolutives et seront régulièrement mises à jour, selon son appréciation des risques que peuvent présenter certaines opérations.

- *Traitements concernés*

  Principalement, les traitements présumés comporter un risque d'atteinte à la protection de la vie privée et des données à caractère personnel, qui s'inscrivent dans l'une ou plusieurs des catégories suivantes :

- traitements qui contreviennent au respect des dispositions de l'article 11 de la loi 09-08, relatif à la neutralité des effets et qui permettent de prendre des décisions sur le fondement d'un traitement automatisé de données à caractère personnel ;

- traitements à grande échelle de données sensibles qui, en vertu de l'article premier de la loi 09-08, révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale de la personne concernée ou qui sont relatives à sa santé y compris ses données génétiques ;

- traitements qui permettent une surveillance systématique des personnes concernées ;

- traitements effectués dans le cadre de l'utilisation de solutions technologiques ou organisationnelles innovantes.

Cette liste s'étend également aux traitements effectués :

- dans le cadre du respect d'une obligation légale à laquelle est soumis le responsable du traitement ;

- dans le cadre de l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

- sur le fondement d'une base juridique qui les réglemente.

Ainsi, une analyse d'impact ne s'avère point nécessaire lorsque la nature, la portée, le contexte et les finalités du traitement envisagé sont très similaires à un traitement pour lequel une analyse d'impact a déjà été menée par le responsable de traitement ou par un tiers (autorités, organismes publics, regroupement de responsables de traitement…), et que ses résultats peuvent être réutilisés et transposés.

Réalisation d'une analyse d'impact

Une analyse d'impact doit être réalisée en amont, dans une logique d'anticipation avant la mise en œuvre du traitement envisagé. Elle doit être revue de manière régulière, afin de s'assurer que le niveau de risque demeure acceptable. Elle peut porter sur une opération ou un ensemble d'opérations de traitement similaires et doit contenir au minimum :

- une description détaillée des opérations de traitement et leurs finalités, comprenant tant les aspects techniques qu'opérationnels ;

- une évaluation, de nature plus juridique, de la nécessité et de la proportionnalité des opérations de traitement au regard des principes et droits fondamentaux (finalité, données et durées de conservation, information et droits des personnes, etc.) non négociables, fixés par la loi et devant être respectés quels que soient les risques ;

- une évaluation de nature plus technique, des risques sur la sécurité des données (confidentialité, intégrité et disponibilité), et leurs impacts éventuels sur la vie privée, qui permet de déterminer les mesures techniques et organisationnelles nécessaires à la protection des données ;

- une description des mesures envisagées pour faire face aux risques (mesures de nature juridique, organisationnelles, de sécurité logique et de sécurité physique), y compris les garanties et mécanismes visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect de la loi.

Acteurs concernés

Le processus de réalisation d'une analyse d'impact doit impliquer l'ensemble des acteurs d'un traitement concerné, à savoir et de manière non exhaustive :

- le responsable de traitement qui est la personne physique ou morale qui détermine la finalité et les moyens du traitement ;

- le ou les sous-traitants qui interviennent dans le traitement, qui doivent fournir leur aide et les informations nécessaires à la réalisation de l'analyse d'impact ;

- les personnes concernées par le traitement, qui peuvent être consultées par le responsable de traitement et formuler leurs avis, notamment par le biais d'une enquête, d'un sondage, d'une question formelle aux représentants du personnel ;

- en fonction du contexte, les métiers (maîtrise d'ouvrage), les équipes chargées de la mise en œuvre (maîtrise d'œuvre), et la personne chargée de la sécurité des systèmes d'information.

La CNDP recommande de renseigner les apports de tous les acteurs sollicités, ainsi que le choix fait de ne point recueillir l'avis d'un acteur particulier.

Une analyse d'impact peut utilement aboutir à la production d'un rapport ou d'un résumé, pouvant être partagé, publié et communiqué. Cette bonne pratique contribue à l'amélioration de la confiance et de la transparence entre les parties prenantes.

Conclusion

Un responsable de traitement peut recourir à la réalisation d'une analyse d'impact pour étayer son dossier de notification. La CNDP, dans sa mission d'accompagnement, et après instruction de la demande soumise, préconisera les mesures à envisager par le responsable de traitement, qu'elle jugera suffisantes pour assurer un niveau de protection des données à caractère personnel adéquat.

Rabat, le 14 décembre 2020
Omar Seghrouchni
Président de la CNDP