COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

ÉTUDE COMPARATIVE SUR LES PROJETS ET RÉALISATIONS

EN MATIÈRE DE CREDIT SCORING EN EUROPE

Septembre 2020

Projet s'inscrivant dans le cadre du Partenariat du voisinage du Conseil de l'Europe avec le Maroc 2018-2021 et financé par la Norvège.

Les vues exprimées dans cette étude sont de la responsabilité des auteurs et ne reflètent pas nécessairement la ligne officielle du Conseil de l'Europe.

Table des matières

Contexte 3
Démarche et méthodologie 3
L'étude 4
1. Définitions des notions de credit scoring, des centrales positives et négatives 4
2.Rappel du référentiel légal 4
3. Le socle commun du RGPD en question, applicable dans les États objets de l'étude 5
4. La nécessaire conciliation entre les règles issues du RGPD et d'autres dispositions contradictoires du droit national 6
5.Observations sur les pratiques dans les pays considérés 7
5. Pratiques et législations pays par pays 7
5.1. Allemagne 8
5.1.1. État des lieux 8
5.1.2. Tendances 9
5.2. Autriche 10
5.2.1. État des lieux 10
5.2.2. Tendances 10
5.3. Belgique 11
5.3.1. État des lieux 11
5.3.2. Tendances 12
5.4. Espagne 12
5.4.1. État des lieux 12
5.4.2. Tendances 13
5.5. Italie 13
5.5.1. État des lieux 13
5.5.2. Tendance 16
5.6. Portugal 16
5.6.1. État des lieux 16
5.6.2. Tendance 17
5.7. Royaume-Uni 17
5.7.1. État des lieux 17
5.7.2. Tendance 18
6. EN CONCLUSION 18

Contexte

Le Conseil de l'Europe met en œuvre un projet de coopération destiné à soutenir le renforcement du droit à la protection des données à caractère personnel au Maroc, en partenariat avec la Commission Nationale de protection des Données Personnelles (CNDP). Dans ce cadre, afin de répondre à la demande d'assistance de la CNDP dans ses réflexions et son adaptation aux développements législatifs, techniques et sociétaux, le Conseil de l'Europe a fait faire un état des lieux analytique des législations et des pratiques en matière de *credit scoring (scores de solvabilité)* dans un nombre de pays européens. Cette étude analyse les dispositifs mis en place dans sept pays de européens (Allemagne, Autriche, Belgique, Espagne, Italie, Portugal et au Royaume Uni) dans la perspective de la dimension protection des données personnelles liée au *credit scoring*.

Cette étude a été confiée au cabinet KPMG Avocats qui avait pour mission de :

- rassembler les exemples de législations et pratiques en matière de *credit scoring* en Allemagne, Autriche, Belgique, Espagne, Italie, Portugal et au Royaume Uni.
- préparer une analyse accompagnée d'un tableau comparatif par pays et des liens hypertexte pertinents en annexe.

Démarche et méthodologie

Les recherches ont été axées sur l'existence de législations et de pratiques dans chacun des pays et attache a été prise avec chaque autorité de contrôle en matière de protection des données personnelles. Toutefois, la plupart n'ont pas répondu ou uniquement oralement.

Les éléments ont été regroupés dans un fichier excel, comprenant un feuillet par pays et permettant de répondre aux questions suivantes :
Si le *credit scoring* est pratiqué dans le pays concerné : Par quel type d'entité ? Sur quelles données ? Comment (listes positives ou négatives, algorithmes et autres modalités de traitement automatisé, si les méthodes sont connues ou non des demandeurs de crédit, etc) ? Est-ce qu'une législation spécifique encadre la pratique ?

Les experts ont également recherché les positions, avis, recommandations des autorités nationales et les ont mentionnés, lorsque cela était opportun, dans le fichier excel.

Une première version du fichier excel a été livrée à la CNDP le 15 septembre 2020pour lui donner un aperçu des travaux en cours. Cette communication n'a pas appelé d'observation.

La version complétée et finalisée du fichier est annexée à la présente étude. Il contient en outre les liens hypertextes pertinents.

L'étude

1. Définitions des notions de credit scoring, des centrales positives et négatives

Dans les différents pays du périmètre géographique de la recherche, l'expression communément utilisée de *credit scoring* recouvre l'ensemble des traitements informatiques de divers renseignements relatifs à un demandeur de crédit afin d'établir une note ou un score indiquant la capacité de cette personne à payer un crédit (ou le risque d'impayé).

Les scores sont susceptibles d'être utilisés comme instrument d'aide à la décision d'octroi ou de refus de crédit mais sont parfois utilisés à d'autres fins, comme une aide à la décision de concéder un bail, ou même une embauche dans une société.

Les renseignements utilisés pour ces scores sont généralement issus soit (i) des informations volontairement communiquées par la personne concernée, soit (ii) figurant dans des fichiers publics et soit (iii) consolidés et/ou obtenus auprès d'entreprises privées.

Les fichiers d'où proviennent les données permettant de pratiquer le *credit scoring*, sont distincts selon que le fichier est positif ou négatif.

Les bases de données sont considérées comme positives et appelées « centrales positives » lorsqu'elles regroupent une pluralité d'informations elles-mêmes positives ou négatives sur la personne concernée afin de déterminer sa capacité de remboursement[1].

Le fichier négatif contient des informations relatives aux incidents financiers de la personne concernée. Ces fichiers désignent les mauvais payeurs ou les fraudeurs.

Enfin un dernier type de fichier existe, il s'agit des listes noires. La personne enregistrée dans un tel fichier se verra exclue de toute obtention de crédit, voire de toute obtention de contrat.

On distingue le *credit scoring* appliqué à des personnes morales ou à des personnes privées.

2. Rappel du référentiel légal

Pour les besoins de l'étude commandée, les experts se sont attachés à cibler les pratiques et législations en vigueur pertinentes pour le *credit scoring* des personnes physiques, étant entendu que la protection des données à caractère personnel touche par définition[2] les personnes physiques.

Sous l'angle des règles applicables à la protection des données à caractère personnel à l'occasion du *credit scoring* :

[1] Le Sénat français dans une note publiée en novembre 2012 avait défini les bases de données positives comme suit : « Les fichiers positifs ou « centrales de crédit positives » ont pour objet de réunir des données permettant de connaître l'endettement d'un emprunteur avant de lui consentir un prêt même s'il n'a pas connu de défaillance dans le remboursement de ses crédits. » http://www.senat.fr/lc/lc231/lc231.pdf

[2] https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679#d1e1559-1-1

(i) la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel modernisée[3] (Convention 108+), fixe les principes de la protection des données ; elle sera applicable à tous ses États parties et reconnue par l'Union européenne comme un élément pris en compte lors des décisions d'adéquation ;

(ii) il y a également un socle commun à chacun des pays membres de l'Union européenne, à savoir le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (« RGPD »).

A ce jour, les initiatives spécifiques et relatives à la protection des données à caractère personnel dans le cadre des activités de *credit scoring*, si elles existent, sont nationales.

3. Le socle commun applicable dans les États objets de l'étude

Les pays visés dans l'étude sont tous Parties à la Convention 108 et, étant membres de l'Union européenne, sont également tous soumis au RGPD, lequel fixe des normes à appliquer en détail.

Dans la perspective qui est celle du Conseil de l'Europe, le référentiel légal est la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel modernisée (Convention 108+) et particulièrement l'article 9[4] ici applicable. Il énonce notamment que :

1. Toute personne a le droit :

a. de ne pas être soumise à une décision l'affectant de manière significative, qui serait prise uniquement sur le fondement d'un traitement automatisé de données, sans que son point de vue soit pris en compte ;

c. d'obtenir, à sa demande, connaissance du raisonnement qui sous-tend le traitement de données, lorsque les résultats de ce traitement lui sont appliqués.

Cet alinéa est précisé au paragraphe 77 du rapport explicatif de la Convention 108+[5]

2. Le paragraphe 1.a ne s'applique pas si la décision est autorisée par une loi à laquelle est soumis le responsable du traitement et qui prévoit également des mesures appropriées pour la sauvegarde des droits, des libertés et des intérêts légitimes de la personne concernée.

S'agissant du RGPD, dans son article 22[6] et exposé dès son considérant 71 il affirme les principes suivants :

[3] Le texte actuellement en vigueur est celui de la Convention 108 de 1981 mais la présente étude se base sur les dispositions de la Convention 108+, disponible à : https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65c0.

[4] https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65c0

[5] https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a

[6] https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679#d1e2884-1-1

« 1. La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

2. Le paragraphe 1 ne s'applique pas lorsque la décision :

a) est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ;

b) est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ; ou

c) est fondée sur le consentement explicite de la personne concernée.

3. Dans les cas visés au paragraphe 2, points a) et c), le responsable du traitement met en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, au moins du droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision.

4. Les décisions visées au paragraphe 2 ne peuvent être fondées sur les catégories particulières de données à caractère personnel visées à l'article 9, paragraphe 1, à moins que l'article 9, paragraphe 2, point a) ou g), ne s'applique et que des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ne soient en place ».

4. La nécessaire conciliation entre les règles de protection des données et d'autres dispositions contradictoires du droit national

Chaque pays semble avoir sa propre interprétation des exigences relevant du cadre de protection des données, telles que la portée de la nécessité d'une information ou la nécessité d'un consentement préalable de la personne concernée lorsque d'autres intérêts concurrents sont prévus par des textes de lois et normes impératives.

En effet, chaque pays est susceptible d'avoir dans son droit positif d'autres pans législatifs qui pourraient être invoqués pour justifier de pratiquer le *credit scoring,* sans pour autant l'autoriser expressément, comme par exemple :

- sous couvert de l'obligation qui est faite aux établissements de crédit de s'assurer de la solvabilité ou de la capacité de remboursement d'une personne physique, dans le cadre de la lutte contre l'insolvabilité et le surendettement ;
- sous couvert du secret bancaire ;
- sous couvert de la lutte contre le blanchiment d'argent ;
- sous couvert de lutte contre la fraude…

Il y a matière à interprétation dans chacun de ces droits sur l'impact de l'existence de ces obligations légales par rapport au respect de la protection des données à caractère personnel.

L'équilibre entre la satisfaction de l'obligation de vérifier la solvabilité avant d'octroyer un crédit, d'une part, et le droit à une transparence ou une information de la personne concernée, d'autre part, est susceptible d'être interprété de manière distincte pays par pays.

Les enjeux porteront notamment sur l'étendue de l'obligation d'informer la personne physique au préalable du fait que des données la concernant seront utilisées aux fins d'établir un *score*, sur la durée de conservation des données et sur l'exercice des droits des personnes concernées (droit d'accès, droit à la rectification notamment, droit à l'effacement, etc.)

La plupart des pays concernés par l'étude n'ont pas une législation suffisamment précise pour encadrer et déterminer les conditions requises pour l'utilisation future des données à des fins de *credit scoring.* Etant donné que, dans les centrales, peuvent figurer des données qui n'ont pas été fournies dans le but de demander un crédit, la qualité de la centrale et la nature de l'entité, publique ou privée, émanation de l'État ou non, qui détient ou compile les données sources qui seront utilisées pour le calcul devient significative[7].

En conséquence, il peut y avoir des variantes entre les législations et pratiques nationales sur les obligations de recueillir le consentement de la personne concernée au préalable lorsque c'est la base légale applicable, les obligations de fournir un accès aux données pour rectification, les obligations de fournir des explications sur la méthode de calcul, les obligations de purge des données et de durées de conservation des entités qui compilent les données dans des centrales, les droits des entités qui pratiquent le calcul à partir de ces centrales, les droits de transmettre à leur tour des données à d'autres pour qu'elles puissent établir leur score.

5. Observations sur les pratiques dans les pays considérés

Les pratiques en matière de *credit scoring* ne sont pas uniformes entre les différents pays étudiés en ce qui concerne les entités qui pratiquent le *credit scoring*, les sources des variables auxquelles elles ont accès et leur qualité (fichiers publics ou non publics, listes positives, listes négatives, listes noires), les données qu'elles collectent et les contraintes et/ou obligations de transparence qu'elles s'imposent.

Les établissements utilisant le *credit scoring* sont soumis à des réglementations propres à leur activité (bancaire, de crédit..) qui peuvent être communes au niveau de l'Union européenne ou comporter des spécificités nationales qui les incitent à vérifier la capacité d'emprunt des demandeurs de crédit ou le risque de non remboursement.

Un état des lieux et des tendances pays par pays pour les territoires concernés par l'étude, les références et les liens hypertextes étant indiqués dans le tableau récapitulatif annexé à la présente consultation sont présents ci-dessous.

5. Pratiques et législations pays par pays

[7] Par exemple, si la personne concernée a un incident de paiement avec son fournisseur d'accès à internet, cette donnée pourra être reprise et compilée dans une centrale qui servira de source pour le calcul du score. La question pourra se poser différemment selon les juridictions de savoir si ladite personne concernée doit dès la conclusion du contrat avec le fournisseur d'accès à internet donner son accord pour que les éventuels incidents de paiement soient répertoriés par un tiers et utilisés ultérieurement ou si la donnée devient publique en raison d'intérêts supérieurs et pour combien de temps cette donnée peut être conservée. Les réponses peuvent différer si l'entité qui compile les données dans la centrale qui sert de base au calcul est étatique ou privée, si la centrale est accessible à tous ou à une liste déterminée d'utilisateurs, si les données sont conservées pour une durée déterminée selon une prescription légale, si la centrale est susceptible de recevoir des demandes d'accès pour rectification ou pour droit à l'oubli.

5.1. Allemagne

5.1.1. État des lieux

(i) Pratique répandue du *credit scoring* par des sociétés privées

En Allemagne, la pratique du *credit scoring* est répandue.

Plusieurs sociétés privées collectent des données et les scores établis sont repris afin d'établir la capacité d'emprunt des personnes physiques lors de l'établissement d'un contrat de crédit ou pour son exécution ou sa résiliation.

Les banques, établissements de crédits et autres sociétés privées (y compris les bailleurs) utilisent principalement le score SCHUFA (établi par la société privée SCHUFA Holding).

Les utilisateurs des scores ne sont pas limités aux établissements de crédits, et peuvent aussi bien concerner d'autres types de créanciers tels que des sociétés de vente à distance ou par correspondance, des bailleurs de biens à usage d'habitation, des fournisseurs d'accès à internet et autres sociétés de communication.

A cet égard, un rapport de synthèse du groupe de travail de la CNIL présidé par Monsieur Philippe Nogrix sur les problèmes posés par les fichiers regroupant des informations sur la situation financière des individus au regard de la loi du 6 janvier 1978 (fichiers dits « centrales positives »)[8] alertait dès 2005 sur les risques relatifs aux pratiques extensives d'utilisation de *credit scoring* concernant l'Allemagne et sur les dérives en cas d'utilisation des scores par des employeurs ou autres entreprises privées.

Il ressort des recherches menées par les experts que ces pratiques sont toujours d'actualité et sont en croissance. Ils ne disposent pas d'élément indiquant que ces pratiques d'utilisation du score de la SCHUFA se soient étendues au « pre-screening [9]» des candidats à l'embauche comme cela peut être le cas dans d'autres pays.

(ii) Utilisation de fichiers positifs et négatifs

La SCHUFA Holding a accès aux informations enregistrées transmises par plus de 7000 entreprises partenaires (banques, caisses d'épargne, sociétés de carte de crédit, sociétés de leasing, entreprises de vente par correspondance, opérateurs de téléphonie mobile, etc).

La liste SCHUFA est une liste positive, elle collecte toutes les informations comptables et financières relatives à une personne. Cependant, à la moindre survenance d'un incident financier, celle-ci devient négative, ce qui influe sur la possibilité pour la personne concernée d'obtenir le crédit souhaité.

[8] https://www.cnil.fr/sites/default/files/typo/document/Rapport-Centrales012005.pdf

[9] Le *prescreening* s'entend comme les vérifications que peut effectuer une personne sur une autre. Dans le contexte de l'espèce, un employeur qui vérifie avant embauche, les historiques des candidats. Les vérifications peuvent aller de la simple consultation du curriculum vitae, à la consultation de ses dettes sur un registre de crédit.

Les autres sociétés pratiquant le *credit scoring* en Allemagne (Bürgel, Dun& Bradstreet, CIG une entreprise fondée par Experian et Credit Reform) constituent également des listes positives pouvant devenir négatives.

(iii) Droit d'accès des personnes concernées limité aux données servant au calcul, et non à la méthode de calcul

Les personnes concernées peuvent en application de l'article 34 du BDSG (loi fédérale sur la protection des données)[10] demander à avoir un accès aux données qui servent au calcul de leur score et demander à les rectifier, gratuitement une fois par an. En revanche, les pratiques des sociétés privées ne semblent pas faire l'objet d'un cadre spécifique régissant les durées de conservation autre que celui de la Convention 108 ou du cadre général du RGPD.

La méthode de calcul des scores n'est pas transparente vis-à-vis des personnes concernées.
La SCHUFA allègue qu'elle est protégée par le secret des affaires.

(iv) Un cadre législatif dérivant du RGPD et néanmoins limité par d'autres dispositions

L'utilisation de moyens automatisés de calcul statistique et mathématique (du type algorithme) est encadrée par la loi fédérale et limitée aux cas de conclusion ou d'exécution de contrats et de manière proportionnée par rapport aux intérêts légitimes de la personne concernée à ne pas faire l'objet d'une décision ou d'une mesure produisant des effets juridiques ou l'affectant de manière significative.

En Allemagne, il semble admis que des limitations et exceptions puissent être apportées aux règles du de protection des données en matière d'information préalable de la personne concernée de l'utilisation qui peut être faite de ses données (hors utilisation limitée aux données personnelles à partir de l'adresse) si une disposition législative impérative contraire existe. A la connaissance des experts, la question de la primauté du droit au respect des règles de protection des données à caractère personnel par rapport à d'autres lois et obligations légales n'a pas encore été tranchée par les tribunaux.

Les banques et établissements de crédit doivent pouvoir justifier de remplir les conditions du RGPD ainsi que des fondements et critères qui les autorisent à ne pas avoir informé de manière préalable les personnes concernées dès lors qu'elles se fondent sur le droit national (ex : lutte contre la fraude fiscale).

5.1.2. Tendances

La commission éthique des données (*Data Ethics Commission*) de l'autorité de protection des données fédérale a émis des recommandations[11]. Elle appelle à une plus grande responsabilisation des banques et établissements de crédit lorsque le *credit scoring* est utilisé de manière équivalente à une intervention humaine.

La commission éthique souhaite que les activités de *credit scoring* des banques et établissements de crédit soient davantage encadrées, que des pistes en ce sens soient explorées par le Gouvernement comme celle d'avoir recours à un label assurant la qualité des algorithmes utilisés afin d'assurer leur fiabilité auprès des personnes concernées, des accréditations par des organisations, ou encore de

[10] https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0294

[11] https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Datenschutz/Data-Ethics-Commission_Opinion.pdf?__blob=publicationFile&v=1

désigner une personne de contact pour les entreprises comme c'est le cas actuellement avec les délégués à la protection des données.

5.2. Autriche

5.2.1. État des lieux

(i) Une utilisation du *credit scoring* par une société privée principalement

En Autriche la pratique du *credit scoring* se fait par des entreprises privées : la principale est le KSV qui se trouve en situation de quasi-monopole et les autres sont le Alpenländischer Kreditorenverband (AKV Europa), Creditreform Wirtschaftsauskunftei Kubicki KG, ou CRIF GmbH (formerly Deltavista).

(ii) Utilisation de centrales positives / négatives et de listes noires

Les données collectées pour les calculs sont relatives à l'identité de la personne et à sa situation financière. L'étendue de ces données est large puisque les études, l'âge des enfants, la profession, le salaire, les dépenses mensuelles ou encore la possession d'une voiture peuvent être traitées.

Il ressort des recherches que plusieurs types de fichiers existent en Autriche puisque le KSV gère des bases de données positives, négatives et des listes noires[12].

(iii) Les pratiques de vérification de solvabilité imposées par la loi et sous contrôle de la FMA

Selon la loi bancaire nationale[13], il pèse sur les établissements bancaires l'obligation de vérifier la solvabilité de leur client. Cette vérification doit être documentée et faire l'objet d'un suivi. Ces mêmes établissements doivent être autorisés par la FMA[14] s'ils veulent offrir un service de classification des risques.
En outre, le droit autrichien en matière de consommation prévoit l'obligation, pour les établissements de crédit aux consommateurs, de vérifier la solvabilité dudit consommateur avant l'octroi d'un crédit. Les établissements de crédit peuvent s'appuyer sur les renseignements fournis par le demandeur de crédit ainsi que sur les éléments figurant sur les bases de données (comme le KKE ou l'indicateur de risque KSV).

(iv) Un cadre relatif à la protection des données personnelles dérivant du RGPD

La loi nationale relative à la protection des données a été grandement modifiée par le RGPD et ne mentionne plus aujourd'hui le *credit scoring*. L'encadrement du traitement des données est assuré par l'application du RGPD.

5.2.2. Tendances

(i) Les enjeux de la portée du droit d'accès des personnes concernées sont débattus

La méthode de calcul automatisée du KSV est opaque et n'est pas communiquée au public.

[12] Source de 2014 https://www.arbeiterkammer.at/infopool/wien/Credit_Scoring_2014.pdf

[13] https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40203208/NOR40203208.pdf

[14] La FMA est une autorité de surveillance des marchés en Autriche créée en 2002. https://www.fma.gv.at/en/financial-market-supervision-in-austria/

Les associations de consommateurs s'inquiètent de cette opacité. La portée du droit d'accès non seulement aux données collectées mais aussi aux méthodes de calcul était déjà une préoccupation avant l'entrée en vigueur du RGPD, y compris devant les tribunaux[15]. Les tribunaux ont en effet régulièrement jugé qu'il pesait, sur les agences de notation, l'obligation d'informer les personnes physiques de leur présence sur la liste d'alerte de manière à permettre aux personnes concernées de rectifier les données utilisées pour le calcul. Plus récemment, les tribunaux administratifs se sont penchés sur l'application de l'article 5 du RGPD dans le cadre de *credit scoring* concernant les finalités, la minimisation des données, la correction et la conservation de données et sur la notion d'intérêt légitime. Ils ont en fonction des faits de l'espèce fait primer les droits des établissements de crédit par rapport aux droits de la personne concernée à faire supprimer les données et estimé une durée de conservation de 5 ans comme étant une durée raisonnable[16].

(ii) L'Autorité de protection des données personnelles autrichienne n'a pas souhaité se prononcer officiellement suite au contact des experts et il n'y a pas eu de retour écrit.

5.3. Belgique

5.3.1. État des lieux

(i) Le *credit scoring* est pratiqué par la Banque Nationale Belge

En Belgique le *credit scoring* est exercé par la Banque Nationale Belge.

Les experts n'ont pas d'information sur l'existence de *credit scoring* par des sociétés privées.

(ii) Coexistence de deux fichiers dits de centrale positive et négative

Afin de procéder au *credit scoring* de personnes physiques, la Banque Nationale Belge puise les données dans deux bases qu'elle gère elle-même. L'une est positive, l'autre est négative.

Selon la base de données, les règles applicables diffèrent. C'est le cas des durées de conservation. Les données figurant dans la liste négative resteront 12 mois après la régularisation de la situation s'opérant par le paiement de la somme demandée. Les données de la liste positive sont quant à elles conservées 3 mois et 8 jours après la fin du contrat auxquelles elles se rattachent.

---

[15] Les tribunaux autrichiens ont dû se prononcer sur des faits remontant à 2015, relatifs aux droits d'accès et de rectification des données utilisées pour évaluer la solvabilité d'un consommateur par une société privée. Un avis de la Commission de protection de 2007 a été cité en première instance sur la portée du droit de recours (comprenant les méthodes de calcul et la qualité de responsable de traitement de celui qui effectue le *credit scoring* dans le cadre d'une demande de crédit). L'affaire est une affaire d'espèce qui a été négociée en appel en 2019. (Datenschutzbehörd 08.02.2016)
https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=d97e9dcf-4e8a-445c-97df-c5559675627e&Abfrage=Gesamtabfrage&SearchInAsylGH=&SearchInAvn=&SearchInAvsv=&SearchInBegut=&SearchInBgblAlt=&SearchInBgblAuth=&SearchInBgblPdf=&SearchInBks=&SearchInBundesnormen=&SearchInDok=&SearchInDsk=&SearchInErlaesse=&SearchInGbk=&SearchInGemeinderecht=&SearchInJustiz=&SearchInBvwg=&SearchInLvwg=&SearchInLgbl=&SearchInLgblNO=&SearchInLgblAuth=&SearchInLandesnormen=&SearchInNormenliste=&SearchInPruefGewO=&SearchInKmGer=&SearchInPvak=&SearchInRegV=&SearchInSpg=&SearchInUbas=&SearchInUmse=&SearchInUvs=&SearchInVerg=&SearchInVfgh=&SearchInVwgh=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=kredit+scoring&Dokumentnummer=DSBT_20160208_DSB_D122_304_0012_DSB_2015_00

[16] https://rdb.manz.at/document/ris.bvwg.BVWGT_20191030_W258_2218465_1_00

D'autre part, l'accès à la liste négative de la Banque Nationale Belge est soumis à la condition d'être sous convention avec cette dernière. Par cette mesure la banque contrôle la confidentialité de la liste et actualise régulièrement la liste des personnes autorisées à consulter la liste négative figurant sur son site internet.

Les données figurant dans ces listes ont attrait à l'identité de la personne, l'état de sa situation financière et sa demande de crédit.

(iii) Un cadre législatif fixé par le RGPD, les règles applicables aux bases de données de la Banque Nationale Belge et les règles figurant dans le code de la consommation

La pratique de la Banque Nationale Belge est encadrée par le RGPD. La Banque est soumise aux lois qui la régule[17] et au code de la consommation[18].

Seules les entités agréées par le Roi des Belges peuvent consulter la centrale. Les données qui sont susceptibles d'être communiquées peuvent être limitées et dans ce cas la consultation n'est pas intégrale. Le Roi définit les types de données qui peuvent figurer dans la centrale. Les personnes concernées ont un accès libre et sans frais à leurs données et peuvent demander rectification. Il n'est pas mentionné de droit à l'oubli.

5.3.2. Tendances

Il ressort des recherches et des échanges avec l'autorité de protection belge que cette dernière n'a pas émis de nouvelle position depuis son dernier avis en date de 2008, et qui avait pour la troisième fois rendu un avis s'opposant à l'utilisation de listes négatives, estimant que le projet de loi encadrant les listes négatives n'était pas suffisamment protecteur.

5.4. Espagne

5.4.1. État des lieux

(i) Une pratique privée du *credit scoring* à partir de bases de données publiques et privées, positives et négatives

Le *credit scoring* en Espagne est opéré par des institutions privées. Il existe des bases de données tant positives que négatives qui servent au *credit scoring* : les sociétés qui pratiquent le *credit scoring* s'alimentent à la fois de données collectées dans des fichiers privés et à partir d'informations figurant dans la centrale positive de la Banque Nationale d'Espagne.

Les données prises en compte sont relatives à l'identification de la personne (nom, adresse, date de naissance, numéro fiscale) et sa situation financière (comportement financier, combien de fois la personne concernée a été inscrite dans un fichier d'insolvabilité).

(ii) Un cadre autorisant l'évaluation de la solvabilité

[17] http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2012030416&table_name=loi
https://www.nbb.be/doc/cr/ccp/kb23032017ckp.pdf

[18] https://www.cecfinance.be/files/conditions%20g%C3%A9n%C3%A9rales/Livre%20VII%20code%20droit%20%C3%A9conomique.pdf

La pratique entourant les bases de données de la Banque d'Espagne fait l'objet de législations notamment sur la transparence et les obligations classiques auxquelles peut être assujettie une banque.

L'article 20 de la loi du 5 décembre 2018[19] relative à la protection des données personnelles définit les conditions d'une présomption de licéité du traitement de données personnelles dans le cadre d'obligations monétaires, financières et de crédit. Cet article précise également les conditions d'application de la présomption de licéité ainsi énoncées ainsi que les qualifications de responsables de traitement selon les cas si l'entité qui collecte les informations est ou n'est pas l'entité qui les traite ou qui les combine avec d'autres sources.

Sans viser expressément le *credit scoring*, le texte semble permettre d'évaluer la solvabilité d'une personne physique à partir d'informations collectées sur son passé et de procéder à des traitements aux fins de déterminer l'octroi d'un crédit. Pour autant il ne dispense pas les entreprises pratiquant l'utilisation des scores de s'assurer de la conformité au RGPD et au respect des durées de conservation et autres obligations.

D'un point de vue général, le recours au *credit scoring* reste limité par le droit au respect de la vie privée et encadré par le RGPD.

(iii) Code de conduite antérieur au RGPD

L'Asnef, qui est une société privée générant des scores, a écrit un code de conduite en 2014[20] sur la gestion de ses fichiers au regard de la protection des données à caractère personnel.

5.4.2. Tendances

L'Autorité de protection espagnole reste très vigilante envers les entités gérant les fichiers de solvabilité. Elles sont souvent pointées du doigt. L'autorité de protection n'encourage pas le traitement d'informations issues de bases de données judiciaires, ou faisant l'objet d'un traitement agressif de type *sentiment analytics* c'est-à-dire axé sur le comportement de la personne, et n'est pas favorable à ce type de traitement sans pour autant les interdire.

5.5. Italie

5.5.1. État des lieux

(i) Pratique du *credit scoring* par des entités privées

L'Italie à recours au *credit scoring* par l'intervention d'agences privées. Les données prises en compte sont multiples et en rapport avec l'identité de la personne, sa situation financière, judiciaire et les modalités de son crédit.

Les agences privées utilisent des données figurant sur une base de données gérée par la Centrale des risques (de la Banque centrale d'Italie) pour plus de 50%, données qu'elles complètent par leur propre base de données et sources d'informations.

[19] https://boe.es/buscar/act.php?id=BOE-A-2018-16673&p=20190625&tn=1#a2-2

[20] https://www.asnefproteccion.es/assets/codigo_tipo.pdf

Dans la pratique, les informations de crédit recueillies par les institutions et agences de crédit peuvent être positives (liste blanche), négatives (liste noire) ou sous le modèle de données complètes (*full data*).

En particulier, le Centre des risques de la Banque d'Italie ne collecte pas lui-même d'informations négatives mais seulement des informations relatives à l'existence de contrats de crédits et de garanties et/ou sûretés prises par l'individu mensuellement. Ce sont les intermédiaires de crédit qui signalent au Centre des risques si la personne physique est un débiteur défaillant (plusieurs retards sur le paiement des dettes) au regard de sa situation financière globale.

(ii) Impératif d'intérêt public de la centrale négative de la Banque Centrale d'Italie

Cette base de données répond à un impératif d'intérêt public et à ce titre le consentement de la personne concernée n'est pas requis.

La Banque centrale d'Italie indique sur son site que les données de la centrale des risques sont confidentielles sans préciser les modalités d'accès des sociétés pratiquant le *credit scoring*.

Le droit d'accès de la personne concernée est gratuit et peut s'effectuer à tout moment.

(iii) Un cadre antérieur au RGPD complexe avec des sources de valeur plus ou moins contraignantes

Comme pour tous les autres pays, la difficulté de la question tient à la pluralité des sources de droit qui la régissent. Des sources de rang constitutionnel aux délibérations du Comité international de la Croix Rouge (CICR), en passant par les circulaires de la Banque d'Italie et de la TUB[21], en passant par les bonnes pratiques et la jurisprudence, plusieurs textes coexistent et sont susceptibles de se contredire.

Depuis novembre 2017, l'échange d'informations a été effectué par l'utilisation d'Internet à la place du réseau interbancaire national (RNI), qui a été progressivement supprimé.

En ce qui concerne les aspects relatifs à la protection de la vie privée des données des clients, en Italie la question est particulièrement tendue entre la protection du crédit et la supervision et la législation visant à protéger les données à caractère personnel.

En effet, depuis l'époque de la loi 675/1996, il y a eu des conflits entre la nécessité du législateur de protéger la vie privée des clients et l'intérêt poursuivi par les intermédiaires financiers.

Plus précisément, le flux d'informations entre les banques (ou les intermédiaires) et la Banque centrale d'Italie représente une communication de données personnelles d'une entité privée à une entité publique.

Les données transférées sont confidentielles et ne peuvent être traitées qu'aux fins de la gestion du risque découlant de l'octroi de crédit.

L'Autorité de protection des données personnelles italienne (il Garante) avait depuis longtemps estimé que « *la divulgation de données à caractère personnel relatives à la dette des clients faite par des intermédiaires financiers au Centre des risques de la Banque d'Italie, comme il est prévu par la loi, n'est pas soumise à l'obligation d'acquisition préalable du consentement de la personne concernée, il est*

[21] *Testo Unico Bancario : https://www.bancaditalia.it/compiti/vigilanza/intermediari/Testo-Unico-Bancario.pdf*

donc interdit d'obtenir la possibilité d'obtenir la suppression des données en l'absence d'une enquête sur l'illégalité, également pour d'autres profils, du traitement ». Le fondement juridique de cette position se trouvait dans l'article 51 et 53 de la TUB, ainsi que l'art. 27 comma 2 de la loi 675/1996.

La situation n'a pas changé avec l'entrée en vigueur du Code de la protection des données à caractère personnel qui a disposé, d'abord à l'article 18, puis à l'article 2-ter à la suite des changements apportés par le décret législatif 101/2018 que le traitement des données à caractère personnel par des entités publiques n'est autorisé que pour l'exercice de fonctions institutionnelles, ce qui, dans le cas de la protection du risque de crédit, est la prérogative de la Banque d'Italie et est expressément prévu dans l'article 53 de la TUB. En outre, l'intérêt public prévu par une source primaire de droit interne, tel qu'établi par le RGDP, est déjà une base juridique valable pour le traitement.

En outre, l'article 2-undecies, d) du nouveau Code de la protection des données à caractère personnel prévoit d'éventuelles restrictions sur les droits des personnes touchées par les articles 15 à 22 du RGPD si le traitement concerne les activités menées par une entité publique « *sur la base d'une disposition législative expresse, à des fins exclusives relatives à la politique monétaire et monétaire, au système de paiement, au contrôle des intermédiaires et au crédit et aux marchés financiers, ainsi qu'à la protection de leur stabilité* » et lorsque cet exercice de droits peut entraîner un préjudice réel et concret pour cette entité.

Par conséquent, cette disposition ne peut pas être invoquée par les intermédiaires, mais il sera nécessaire, au cas par cas, d'équilibrer les besoins de l'ancien article 47 de la Constitution avec les libertés et les droits garantis par l'ensemble des dispositions réglementaires pour protéger les données à caractère personnel.

En outre, en application du paragraphe 3 suivant du Code, la personne concernée peut toujours exercer les droits prescrits par le RGPD, par l'intermédiaire du Garant, en vertu de l'article 160 du Code si ces limitations dans la manière dont elles sont communiquées, constituent une limite à ses intérêts légitimes et vont à l'encontre de l'objet des limitations.

Des mécanismes antérieurs à l'entrée en vigueur du RGPD[22] permettaient et encadraient la possibilité de rectifier les données détenues par le Centre des risques, une fois que les règlements avaient lieu.

Enfin, il convient de noter que, de toute façon, les intermédiaires peuvent consulter les archives du risque central de la Banque d'Italie uniquement pour la période des 36 derniers mois, avec des avantages évidents pour les personnes concernées.

La doctrine italienne[23] a débattu de la question de l'application des règles relatives à la relation « banque – client » aux rapports (et aux scores) qui seraient erronés afin d'assurer un « droit à

[22] l'art. 8 bis de D.L. 70/2011, modifié par l'art. 3, paragraphe 12 bis, lett. a), D.L. 13 août 2011, no 138 et, enfin, art. 22, paragraphe 6 bis, D.L. 24 juin 2014, n. 91, ont introduit des moyens de rectifier les rapports négatifs sur les particuliers et les personnes morales : au premier alinéa de cette règle, En effet, on s'attend à ce que « *dans les dix jours suivant la réception de la notification de la régularisation des paiements, les gestionnaires des bases de données complètent les rapports de retards de paiement par les personnes ou les personnes morales déjà inscrites dans les bases de données elles-mêmes avec la notification du paiement par le créancier bénéficiaire du paiement, qui doit prévoir la demande dans un délai de quinze jours au plus tard après le paiement a eu lieu* ». Les mêmes considérations s'appliquent aux paiements de versements mensuels et aux régularisations par paiement subséquentes.

[23] G. Biferali, *Big data e valutazione del merito creditizio per l'accesso al peer to peer lending*, dans *Dir. Informatica*, II, 3, 1 juin 2018, 487 ss ; cité par https://www.iusinitinere.it/il-credit-reporting-e-il-credit-scoring-nellera-del-gdpr-16810

rectification » aux clients. Il en ressort que l'activité de collecte et de transmission d'informations aux bases de données par les intermédiaires, relevant de la relation banque-client, reste soumise aux principes qui en régissent l'exercice. Ainsi la banque qui a recours à une méthode de *credit scoring* pour évaluer la possibilité d'octroyer un prêt, devrait ainsi se conformer aux règles relatives à la protection du consommateur dans sa relation avec le banquier.

5.5.2. Tendance

(i) Elaboration d'un code de conduite avec les professionnels du *credit scoring* et implémentation à venir

Des professionnels effectuant le *credit scoring* ont mis en place un code de conduite, le 12 septembre 2019[24], qui a fait l'objet de l'approbation du Garant de la protection des données à caractère personnel italien. Le code de conduite comprend notamment des mesures concrètes visant une protection efficace des données et préconise la mise en place d'une autorité de contrôle qui va vérifier la bonne application des mesures du code.

Le Garant de la protection des données à caractère personnel italien recommande que ladite autorité de contrôle soit indépendante. L'autorité n'a pas encore été désignée.

5.6. Portugal

5.6.1. État des lieux

(i) Une utilisation par les établissements financiers privés

Le *credit scoring* est pratiqué au Portugal par les institutions financières qui accordent des crédits, crédits-bails, ou encore pratiquant l'affacturage. De même, certaines entreprises du secteur privé ou autres entités se servent de ces scores dans le cadre de leurs activités commerciales. Suite à un contact auprès de la Banque du Portugal, elle affirme ne pas pratiquer de *credit scoring* pour les particuliers mais collecte simplement des données au sein de son registre central des crédits.

Les informations utilisées pour ces scores sont contenues dans des bases de données comportant à la fois des informations sur le passé contractuel et les incidents de paiement. Ces dernières sont gérées par les institutions financières.

Outre la confidentialité, la base de données est également soumise au principe de réciprocité selon lequel toute entité ayant accès à la base de données et qui récupère des informations doit en retour alimenter elle-même la base.

(ii) Maintien des autorisations rendues avant l'entrée en vigueur du RGPD par la Commission nationale de protection des données

Les décisions d'autorisation de traitements rendues par l'autorité de contrôle portugaise (CNDP) antérieurement à l'entrée en vigueur du RGPD continuent de s'appliquer dès lors que les traitements considérés sont les mêmes.

[24] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9141941

5.6.2. Tendance

La CNPD accepte la génération de scores à partir de l'information des entités participant à la base de données, à condition que les entités participantes ne fondent pas leur décision seulement sur le score et que les personnes concernées soient informées de cette activité et qu'on leur ait fourni des informations pertinentes sur la logique appliquée au *credit scoring* ainsi que les conséquences envisagées d'un tel traitement.

5.7. Royaume-Uni

5.7.1. État des lieux

(i) Une utilisation privée du *credit scoring*

Au Royaume-Uni le *credit scoring* est pratiqué par des entreprises privées appelées agences de crédit dont trois majeures qui sont contrôlées par la *Financial Conduct Authority* en charge de réguler les entreprises financières et les marchés financiers.

Au regard de la méthode employée pour le calcul des scores, chaque agence de crédit a sa méthode et il n'en existe pas de générale. Ainsi, les données utilisées ne seront pas nécessairement les mêmes d'une agence à une autre.

Les utilisateurs des scores ne sont pas limités aux seuls établissements de crédit. Les employeurs et les sociétés privées peuvent utiliser les scores dans le cadre de *pre-screening* [25]. Dans le cadre d'une offre d'emploi, l'employeur peut consulter le score du candidat et refuser le poste en cas de mauvais score. Le score d'un travailleur indépendant affecte son activité commerciale dès lors qu'il souhaite emprunter de l'argent pour le bien de sa profession.

Les données peuvent également être utilisées dans le cadre de marketing direct et de prospection.

(ii) Une activité peu réglementée

L'activité de *credit scoring* des individus ne fait pas l'objet d'une réglementation spécifique et le droit commun s'applique.

La loi de 2018 sur la protection des données personnelles[26] ainsi que le RGPD régissent les traitements opérés sur les données. A la date de cette étude, en raison du Brexit, le droit positif britannique fait l'objet d'une revue intégrale et la période transitoire d'application du RGPD est censée se terminer le 31 décembre 2020.

[25] Dès 2005 la CNIL faisait un état des lieux de l'existence de technique de pré-sélection et de pre-screening dans le cadre de prospection commerciale donnant lieu à des crédits pré-approuvés. https://www.cnil.fr/sites/default/files/typo/document/Rapport-Centrales012005.pdf. En 2011 L'ICO a publié un guide pratique autour de l'emploi et émet des recommandations quant à cette pratique. https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

[26] https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

5.7.2. Tendance

(i) Une volonté d'encadrement par les utilisateurs des scores, et d'auto-régulation de l'industrie

Il est à noter que compte tenu de l'actualité croissante sur les questions de sécurité des bases de données, dans le domaine bancaire et financier notamment, des efforts de communication au grand public sur les pratiques de *credit scoring* sont faites dans des termes généraux.

Une note d'information de référence *CRAIN* précise comment les agences de crédit collectent et traitent les données utilisées pour le score.

De plus, l'autorité de protection des données (Information Commissioner Office) a publié un guide expliquant ce qu'est le *credit scoring*, comment il s'opère et quels sont les droits des personnes concernées vis à vis de leurs données.

Dans le détail, en revanche, les méthodes utilisées (les algorithmes) pour aboutir au score ainsi que les variables et données utilisées pour le calcul demeurent opaques et rien n'oblige à ce jour les établissements de crédit à les dévoiler.

Cette situation s'explique par la diversité des méthodes utilisées par les agences de crédit et par les établissements de crédit eux-mêmes et du fait que les algorithmes et méthodes de calcul du risque de prédiction de la capacité de remboursement (binaires ou non) peuvent être couverts par le secret des affaires.

Les établissements de crédit peuvent ainsi utiliser leur propre méthode de *credit scoring*, sans avoir d'obligation d'indiquer les seuils maximum ni minimum pour pouvoir accéder au crédit, ni devoir justifier le refus d'un crédit.

La *Finance and Leasing Association* milite cependant pour plus de transparence et sur l'importance d'indiquer aux consommateurs une motivation satisfaisante en cas de refus de crédit, et si le refus a été motivé par un score, quel est le nom de l'agence de notation qui a été impliquée pour l'établissement dudit score.

(ii) Un sujet en suspens du fait de l'actualité

Les experts n'ont pas eu de retour particulier de l'autorité de protection (ICO) sur les perspectives d'évolution de la réglementation spécifique dans le cadre du *credit scoring* en ce qui concerne l'application des règles de protection des données à caractère personnel.

Les travaux actuels de l'ICO sont majoritairement concentrés sur les conséquences du Brexit.

6. EN CONCLUSION

Cette étude a été finalisée le 30 septembre 2020 à partir des informations disponibles et des entretiens téléphoniques et échanges par courriel avec les entités et autorités qui ont bien voulu répondre aux questions des experts.

Il est à noter que l'intervention de la Convention 108 modernisée et du RGPD dans le dispositif législatif des pays concernés par l'étude est encore récente et que les pratiques, les dispositions législatives et réglementaires et les jurisprudences de chacun de ces pays sont susceptibles d'évoluer.

Comme évoqué, les pratiques sont variées et les intérêts en jeu évalués au cas par cas. Les interprétations données dans les pays s'appuient sur la nature des intérêts défendus (utilisation du *credit scoring* par des entités privées ou étatiques dans le cadre d'un intérêt légalement prévu comme impératif).

Il ressort des observations des experts qu'il n'y a pas de position figée sur l'arbitrage à effectuer entre le respect du droit à la protection des données le respect de la défense des intérêts des banques ou établissements de crédit qui pratiquent le *credit scoring*. Cela a des conséquences sur le choix de la base légale du traitement et sur l'application du principe de finalité explicite, déterminée et légitime.

L'opinion publique, les associations de consommateurs et certaines autorités poussent cependant à une plus grande transparence, en conformité avec les articles 8 et 10 de la Convention 108 modernisée, notamment sur le recours aux analyses d'impact et à des mesures découlant de la vie privée dès la conception (*privacy by design*) – et à une responsabilisation accrue des établissements de crédit et autres utilisateurs des scores.
En effet, elles estiment que les établissements de crédit se doivent de rendre des comptes aux personnes physiques pour leur permettre non seulement d'accéder aux sources pour les rectifier mais aussi d'informer les personnes physiques qu'elles font l'objet d'une décision prise en fonction d'une pratique du *credit scoring,* de la transparence sur la méthode utilisée, les modes de pondération. Leur souhait se heurte encore à présent à des dispositions législatives complexes mêlant protection du secret des affaires, obligation de vérifier la solvabilité des emprunteurs dans le cadre de la lutte contre le surendettement et secret bancaire pour ne citer qu'eux.

Hormis au Royaume-Uni où l'utilisation des scores est très large et va au-delà de la demande d'obtention de crédit, les pays civilistes semblent vouloir encadrer strictement les accès aux centrales pour en limiter le nombre d'utilisateurs et restreindre la pratique du *credit scoring* à des fins d'obtention de crédit.

Dans l'ensemble, les règles du droit à la protection des données semblent être progressivement intégrées et mises en œuvre dans les pratiques mais une certaine opacité perdure.

* * *

ANNEXE :

fichier excel - tableau récapitulatif pays par pays avec les liens hypertexte pertinents