RB PRESSE

BANQUE & DROIT

n° 176
Novembre-décembre 2017
ISSN 1777-5752
Bimestriel 70 euros
revue-banque.fr

la pratique du droit bancaire et financier et de la conformité

RB REVUE BANQUE

Nouveau cadre juridique pour les traitements de lutte contre la fraude externe dans le secteur bancaire et financier

FLORENT GASTAUD

Data Protection Officer (DPO) OVH Group

Publiée trois années après l'AU-39, autorisation unique de traitements de données à caractère personnel ayant pour finalité la lutte contre la fraude dans le secteur assurantiel, une autorisation unique similaire, l'AU-054 a été publiée en juillet dernier pour le secteur bancaire et financier. Particulièrement détaillée, celle-ci comporte de nombreux garde-fous, obligeant les entités concernées à encadrer et sécuriser leurs traitements de lutte contre la fraude. En outre, malgré des finalités quasi identiques (lutte contre la fraude), et dans un contexte sectoriel très similaire (banque/assurance), l'autorisation unique du secteur bancaire et financier se veut plus restrictive tout en étant plus contraignante que l'AU-39.

Trois ans après avoir autorisé le secteur assurantiel à mettre en œuvre des traitements de lutte contre la fraude dans le cadre d'une autorisation unique n° 039[1] (AU), la Commission nationale de l'informatique et des libertés (CNIL) vient d'adopter une nouvelle autorisation très similaire pour le secteur bancaire et financier. Publiée au Journal officiel le 25 juillet 2017, l'autorisation unique n° 054[2] vient ainsi grandement simplifier la mise en œuvre de traitements ayant pour finalité la lutte contre la fraude externe et mixte au sein du secteur bancaire et financier.

Préalablement à cette autorisation unique, chaque entité du secteur devait en effet obtenir une autorisation émanant de la CNIL – dont la délivrance prend souvent plusieurs mois – afin de mettre en œuvre un traitement de lutte contre la fraude. En effet, un tel traitement de par sa nature même, impliquait quasi systématiquement l'interconnexion de fichiers dont les finalités principales sont différentes (passation, gestion et exécution des contrats ; gestion du personnel ; gestion des prestataires ; gestion des procédures amiables et contentieuses, gestion de la fraude, etc.) et/ou l'exclusion des fraudeurs avérés du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire. Or la mise en œuvre de traitement remplissant les critères suscités est soumise à autorisation préalable de la CNIL en vertu de l'article 25 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés[3].

Et bien que les traitements de lutte contre la fraude ne soient pas directement des obligations légales (tant pour le secteur assurantiel que celui bancaire et financier), il est indéniable que ces traitements constituent une absolue nécessité pour les entités de ces secteurs. Outre protéger la rentabilité des entités concernées, ces traitements ont un objectif plus global : celui de protéger le système financier. En outre, ces traitements permettent de répondre de manière plus indirecte à des obligations incombant aux entités des secteurs concernés :

– d'une part, les traitements de lutte contre la fraude permettent régulièrement de détecter des activités frauduleuses pouvant avoir un lien direct avec des activités de blanchiment et de financement du terrorisme ;

– d'autre part, les risques de fraude constituent des risques opérationnels devant être identifiés au sein des dispositifs de contrôle interne garantissant la surveillance et la maîtrise des risques des entités des secteurs assurantiel, bancaire et financier.

1. Délibération n° 2014-312 du 17 juillet 2014 portant autorisation unique de traitements de données à caractère personnel ayant pour finalité la lutte contre la fraude à l'assurance mis en œuvre par les organismes d'assurance, de capitalisation, de réassurance, d'assistance et par les intermédiaires d'assurance (AU 039) : https ://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000029312069.
2. Délibération n° 2017-217 du 13 juillet 2017 portant autorisation unique de traitements de données à caractère personnel aux fins de la lutte contre la fraude externe dans le secteur bancaire et financier (AU-054) : https ://www.legifrance.gouv.fr/affichTexte.do;jsessionid=857BB1BACDAD95675683279A1A32E7E6.tpdila17v_2?cidTexte=JORFTEXT000035268554&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000035268151.
3. Article 25 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés : https ://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=72A4AC5735CAEC3CFD05A98D04F9E565.tpdila17v_2?idArticle=LEGIARTI000006528109&cidTexte=LEGITEXT000006068624&dateTexte=20080609.

Compte tenu de la nécessité évidente pour les entités du secteur bancaire et financier de mettre en œuvre des traitements de lutte contre la fraude, certaines entités avaient d'ores et déjà réalisé et obtenu des autorisations de mise en œuvre auprès de la CNIL. C'est notamment le cas du Crédit Mutuel Arkéa (novembre 2014[4]), de la Banque Populaire Provençale et Corse (juillet 2015[5]) ou encore du Crédit Agricole d'Aquitaine (septembre 2015[6]). Or, dans ces trois cas comme dans la majorité des autorisations délivrées, le périmètre des traitements autorisés était relativement restreint puisque limité à la lutte contre la fraude à l'identité ou plus précisément « *à détecter les documents présentant des anomalies susceptibles de révéler une fraude (faux document ou document falsifié) au moment de l'entrée en relation du client auprès de la banque, en cas de modifications de données du compte existant* », « *et lors de contrôles menés postérieurement à l'ouverture du compte* ». Nul doute que certaines entités mettaient par ailleurs en œuvre des traitements de lutte contre la fraude de manière illégale, c'est-à-dire sans avoir obtenu préalablement une autorisation de la CNIL.

Disposer d'un cadre sectoriel, simplifié et harmonisé en matière de traitements de lutte contre la fraude, était donc particulièrement pertinent. C'est d'autant plus vrai que la CNIL est engagée depuis plusieurs années – une concertation s'est ouverte le 6 octobre 2014 à cet effet – avec les professionnels du secteur bancaire et financier dans l'élaboration d'un « *pack de conformité banque* » destiné à regrouper des normes simplifiées et autorisations uniques. L'intérêt est double : harmoniser à l'ensemble des acteurs d'un secteur d'activité la doctrine de la CNIL au regard de leurs spécificités tout en allégeant les formalités préalables de ceux-ci. Bien qu'ayant pris du retard sur le secteur assurantiel, dont le pack de conformité fut finalisé et publié en juillet 2014, le secteur bancaire comble progressivement ses lacunes avec pas moins de six délibérations spécifiques à son secteur :

– AU-003 relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme[7] ;

– AU-005 relative à l'évaluation et à la sélection des risques en matière d'octroi de crédit[8] ;

– AU-045 relative à la consultation du répertoire national d'identification des personnes physiques (RNIPP)[9] ;

– AU-054 relative à la lutte contre la fraude externe ;

– NS-012 relative à la tenue des comptes de la clientèle et le traitement des informations s'y rattachant[10] ;

– NS-013 relative à la gestion des crédits ou des prêts[11].

Notons tout de même que les normes simplifiées 12 et 13 sont particulièrement anciennes, puisqu'elles datent respectivement des années 1980 et 1988 et qu'elles ne répondent plus réellement aux enjeux actuels.

Le secteur bancaire et financier ayant de fortes similitudes avec le domaine assurantiel, il est intéressant de constater que l'AU-054 récemment publiée et relative à la lutte contre la fraude externe dans le domaine bancaire et financier présente logiquement des similitudes avec l'AU-039 relative à la lutte contre la fraude dans le secteur assurantiel. Pourtant, la nouvelle AU-054 du secteur bancaire et financier se veut bien plus complexe dans sa rédaction – neuf pages de délibération contre quatre pour le secteur assurantiel – tout en étant plus restrictive. Un paradoxe qui démontre certainement à lui seul la complexité des échanges entre la CNIL et les acteurs privés dans la rédaction de ce type de texte.

Un champ d'application limité

L'autorisation unique n° 054 est applicable à l'ensemble des entités régulées par l'ACPR et visées au livre V du Code monétaire et financier[12], ainsi qu'aux filiales contrôlées par ces entités exerçant une activité qualifiée de « connexe ». Sont ainsi notamment concernés les établissements de crédit, les intermédiaires en opérations de banque, les conseillers en investissement, sociétés de financement, etc.

Ces entités peuvent adresser un simple engagement de conformité à la CNIL dès lors qu'elles mettent en œuvre un traitement respectant l'ensemble des dispositions de l'AU-054. Ce traitement ne pourra concerner que la détection ainsi que la qualification des anomalies et la gestion des opérations qualifiées de fraude externe et mixte de services bancaires et financiers.

La notion de « fraude externe » est définie par renvoi à un règlement[13] comme étant toutes « *pertes liées à des actes de tiers visant à commettre une fraude ou un détournement d'actif ou*

4. Délibération n° 2014-462 du 13 novembre 2014 autorisant le CREDIT MUTUEL ARKEA à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité de lutter contre la fraude à l'identité : https ://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000029998174&fastReqId=1962612744&fastPos=54.
5. Délibération n° 2015-238 du 9 juillet 2015 autorisant la Banque Populaire Provençale et Corse à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la lutte contre la fraude à l'identité : https ://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000031248916&fastReqId=1962612744&fastPos=22.
6. Délibération n° 2015-280 du 10 septembre 2015 autorisant le Crédit Agricole d'Aquitaine à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la lutte contre la fraude à l'identité : https ://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000031307406&fastReqId=1962612744&fastPos=19.
7. Délibération n° 2011-180 du 16 juin 2011 portant autorisation unique de traitements de données à caractère personnel mis en œuvre par des organismes financiers relatifs à la lutte contre le blanchiment de capitaux et le financement du terrorisme ainsi qu'à l'application des sanctions financières : https ://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000024323084.
8. Délibération n° 2008-198 du 9 juillet 2008 modifiant l'autorisation unique n°AU-005 relative à certains traitements de données à caractère personnel mis en œuvre par les établissements de crédit pour aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit : https ://www.legifrance.gouv.fr/jo_pdf.do?numJO=0&dateJO=200808 05&numTexte=41&pageDebut=&pageFin=.
9. Délibération n° 2015-229 du 9 juillet 2015 portant autorisation unique de traitements de données à caractère personnel aux fins de consultation du répertoire national d'identification des personnes physiques (RNIPP) mis en œuvre par les établissements du secteur bancaire et financier soumis aux obligations relatives aux comptes bancaires inactifs et des coffres inactifs ou par une personne mandatée à cet effet (AU-045) : https ://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000031415436.
10. Délibération n° 80-22 du 8 juillet 1980 concernant les traitements automatisés d'informations nominatives relatifs à la tenue des comptes de la clientèle et le traitement des informations s'y rattachant par les établissements bancaires et assimilés : https ://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017654312.
11. Délibération modifiée par les délibérations n° 85-14 du 30 avril 1985 et n° 88-82 du 5 juillet 1988, concernant les traitements automatisés d'informations nominatives relatifs à la gestion des crédits ou des prêts consentis à des personnes physiques par les établissements de crédit : https ://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017654315&fastReqId=2084275683&fastPos=14.
12. Livre V du Code monétaire et financier : « Les Prestataires de services » : https ://www.legifrance.gouv.fr/affichCode.do;jsessionid=20B69B92F0C6D4AB77D8895ACFB2987A.tpdila17v_2?idSectionTA=LEGISCTA000006123943&cidTexte=LEGITEXT000006072026&dateTexte=20170822.
13. Article 324 du Règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012 : http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A32013R0575.

à enfreindre/tourner la loi ». La notion de « *fraude mixte* » est-elle définie par la CNIL comme étant de la « *fraude externe intervenant avec la complicité d'un collaborateur de l'entité* ». Notons donc à la lecture de ces définitions que le terme de « fraude » n'est en lui-même pas défini au sein de cette AU.

En tout état de cause, le champ d'application de l'autorisation unique du secteur bancaire et financier se veut d'entrée de jeu plus restrictif que celui du domaine assurantiel. En effet, il ne concerne pas la fraude interne, c'est-à-dire celle impliquant uniquement des salariés de l'entité concernée. A contrario, l'AU-39 du secteur assurantiel prévoyait bien dans son champ d'application la mise en œuvre de traitements relatifs à la lutte contre la fraude interne, bien que ce soit dans le cadre exclusif de requêtes individuelles et ponctuelles. C'est d'ailleurs cette même restriction qui est reprise au travers de l'AU-54 du secteur bancaire et financier en matière de traitement des données du personnel dans le cadre du traitement de fraude mixte.

En raison de ce champ d'application restreint, il est fort probable que de nombreuses entités du secteur bancaire et financier soient amenées à devoir réaliser des demandes d'autorisations, en parallèle de leur engagement de conformité à l'AU-054, pour leurs traitements relatifs à la lutte contre la fraude interne. Certaines entités avaient d'ailleurs d'ores et déjà obtenu une telle autorisation, à l'image de BARCLAYS BANK PLC (juin 2015[14]), autorisée à mettre en œuvre un traitement de lutte contre la fraude interne basé sur un outil déclenchant des alertes sur la base d'opérations financières ou administratives réalisées par un collaborateur de l'entité sur des comptes bancaires de clients.

Autre limitation notable : l'AU-054 exclut la gestion des procédures amiables et contentieuses consécutives à un cas de fraude. La CNIL incite à cet effet les entités du secteur bancaire et financier à séparer leurs traitements de lutte contre la fraude externe (AU-054) de ceux de gestion de leurs contentieux (AU-046[15]). Une exclusion difficilement justifiable lorsque le secteur assurantiel bénéficie quant à lui de la possibilité d'incorporer des données relatives aux procédures amiables et contentieuses dans les traitements mis en œuvre dans le cadre de l'AU-39 relative à lutte contre la fraude.

La possibilité de mutualiser les traitements de lutte contre la fraude au sein d'un groupe

C'est l'un des intérêts majeurs de cette autorisation unique 054, à savoir permettre aux entités d'un même groupe de partager les informations relatives aux fraudeurs avérés identifiés au niveau du groupe.

L'AU-054 laisse la possibilité aux groupes concernés de choisir entre deux modes de partage de leurs données relatives à la lutte contre la fraude. En toutes circonstances, ces partages doivent respecter le secret professionnel défini dans le Code monétaire et financier[16] :

– option 1 : un partage ponctuel de données ;

– option 2 : une mutualisation intragroupe des données relatives aux auteurs de fraudes avérées et à leurs victimes.

Ce choix doit être opéré au niveau du groupe eu égard à « l'activité et à l'organisation » des entités d'un même groupe.

En pratique, la seconde option devrait très largement être privilégiée par les entités du secteur bancaire et financier. C'est en effet celle qui facilitera réellement les actions menées en matière de lutte contre la fraude au sein des groupes concernés. C'est notamment grâce à la création d'une base mutualisée entre les entités d'un même groupe qu'il sera possible d'opérer une vérification de la présence ou de l'absence d'inscription d'un futur client, lors de son entrée en relation, au sein du traitement mutualisé des fraudeurs avérés recensés par le groupe. En cas d'occurrence, une vérification manuelle pourra alors être déclenchée par les équipes en charge de la lutte contre la fraude et donner lieu, si cela est justifié, au refus d'entrée en relation contractuelle.

Notons que l'AU-054 encadre très largement le recours à cette option n° 2 en la soumettant au respect d'un grand nombre d'exigences organisationnelles et de sécurité informatique (notamment, chaque entité étant la source des données doit conserver la maîtrise des dites données déversées au sein du fichier mutualisé). De telles précautions n'avaient pas été prises dans l'autorisation unique relative au secteur assurantiel, qui prévoit sans plus de précisions, la possibilité à un responsable de traitement de réaliser des interconnexions de données avec ses traitements et ceux du groupe auquel il appartient.

Notons enfin qu'en toute logique, il ne sera pas possible aux bancassureurs de mutualiser les traitements de lutte contre la fraude qui concernent d'une part leurs entités d'assurance au sens de l'AU-039 et d'autre part leurs entités bancaires au sens de l'AU-054.

L'obligation de mettre à disposition de la CNIL une liste des critères et des scénarios utilisés à des fins de détection de la fraude externe

Outre réaliser un engagement de conformité à l'AU-054, les entités concernées devront également maintenir à jour la liste des critères et des scénarios utilisés à des fins de détection de la fraude externe. En pratique, les entités concernées devront donc définir des critères de suspicion de fraude ainsi que les procédures de détermination des fraudes avérées, de telle sorte à objectiver toute prise de décision en la matière.

Pour ce faire, les entités peuvent compter sur la possibilité de traiter un grand nombre de données dont les catégories sont listées au sein de l'AU-054. L'une d'entre elle est particulièrement notable puisqu'elle concerne « *les données de navigation et de connexion aux systèmes d'information [...] collectées dans le cadre des contrats souscrits [...]* », incluant de ce

---

14. Délibération n° 2015-207 du 25 juin 2015 autorisant BARCLAYS BANK PLC à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la lutte contre la fraude interne des salariés : https ://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000031174414&fastReqId=823627738&fastPos=2.

15. Délibération n° 2016-005 du 14 janvier 2016 portant autorisation unique de traitements de données à caractère personnel mis en œuvre par les organismes publics et privés pour la préparation, l'exercice et le suivi de leurs contentieux ainsi que l'exécution des décisions rendues (AU-046) : https ://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032037367.

16. Article L511-33 du Code monétaire et financier : https ://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006072026&idArticle=LEGIARTI000021762030&dateTexte=&categorieLien=id.

fait des données telles que la géolocalisation ou encore des données émanant de cookies ou autres traceurs. Cette catégorie de données, tout en restant limitative, illustre la bonne prise en compte par la CNIL des nouvelles technologies, et tend à imiter l'AU-039 qui autorisait par renvoi à la NS-56[17] les entités assurantielles à traiter des données « *de localisation et de connexion* » dans le cadre de leurs traitements de lutte contre la fraude.

L'obligation de réaliser des études d'impact sur la vie privée (EIVP) sous certaines conditions

Autre obligation à la charge des responsables de traitement souhaitant bénéficier du cadre de l'AU-054 : l'obligation de réaliser des études d'impact sur la vie privée (EIVP) pour tout scénario de fraude non-expressément listé au sein de l'autorisation unique. Fort heureusement, ces scénarios sont relativement étendus puisqu'ils englobent la fraude aux moyens de paiement, monétique, documentaire et identitaire, au crédit/leasing/location longue durée, à l'affacturage, ainsi que toutes fraudes visant les clients ou l'entité. Notons que cette dernière catégorie « balai » pourrait permettre d'englober de nombreuses typologies de fraude et ainsi limiter les cas pratiques pour lesquels une étude d'impact sur la vie privée serait réellement obligatoire.

L'intégration du mécanisme des EIVP par la CNIL est une anticipation de l'entrée en vigueur, le 25 mai 2018, du Règlement général sur la protection des données (RGPD). Ce dernier prévoit[18] notamment que « *l'autorité de contrôle établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise* ».

Un délai de qualification des alertes plus important que dans le secteur assurantiel

L'AU-054 prévoit un délai maximal de qualification des alertes de suspicion de fraude de 12 mois à compter de leur émission. Une fois ce délai passé, toute alerte non qualifiée ou qualifiée de non pertinente doit être supprimée sans délai.

Ce délai, le double de celui prévu pour le secteur assurantiel (6 mois), est difficilement justifiable. En pratique, ses effets restent limités puisque tant les entités relevant de l'AU-054 que de l'AU-039 pourront conserver les alertes qualifiées de pertinentes durant un délai de 5 années à compter de la clôture du dossier de fraude. Or, aucun délai n'est imposé pour aboutir à la clôture des dits dossiers.

Un mécanisme de double information des personnes concernées

Le mécanisme d'information des personnes concernées par le traitement de lutte contre la fraude est quasiment calqué sur celui de l'autorisation unique du secteur assurantiel. Il s'opère à un double niveau :

– préalablement au traitement : les personnes dont les données sont collectées sont informées de l'existence d'un traitement de lutte contre la fraude. En pratique, cette information sera la plupart du temps fournie dans les documents remis par l'entité lors de la souscription d'un contrat ;

– en cas de confirmation d'une anomalie produisant des effets juridiques suite à investigation humaine : la personne concernée doit être en mesure de présenter ses observations tout en étant informée qu'elle est susceptible d'être inscrite sur une liste de personnes présentant un risque de fraude.

En résumé

Dans le cadre de ses travaux visant à simplifier la mise en œuvre de traitements sectoriels dont les finalités sont considérées comme légitimes, la CNIL, suite à concertation avec les professionnels du secteur bancaire et financier, a abouti à la rédaction de l'autorisation unique 054 le 13 juillet 2017, relative à la lutte contre la fraude externe. Cette dernière est particulièrement détaillée et comporte à ce titre de nombreux garde-fous, obligeant les entités concernées à particulièrement encadrer et sécuriser leurs traitements de lutte contre la fraude.

Son périmètre restreint ne permettra certainement pas d'atteindre les objectifs escomptés, puisque les entités du secteur devront, dans la plupart des cas, réaliser des demandes d'autorisations préalablement à la mise en œuvre de leurs traitements relatifs à la lutte contre la fraude interne.

Publiée trois années après l'AU-39, spécifique au secteur assurantiel, l'AU-054 comporte de nombreuses différences avec sa grande sœur. Alors que les finalités de ces autorisations sont quasi-identiques (lutte contre la fraude), et ce dans un contexte sectoriel très similaire (banque/assurance), l'autorisation unique du secteur bancaire et financier se veut plus restrictive tout en étant plus contraignante. Cette différence est sans aucun doute la marque d'une évolution de l'Autorité de contrôle, créant ainsi une certaine différence de traitement entre le secteur assurantiel d'une part, et bancaire et financier d'autre part. ■

17. Délibération n° 2013-213 du 11 juillet 2013 portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion commerciale de clients et de prospects mis en œuvre par les organismes d'assurance, de capitalisation, de réassurance, d'assistance et par les intermédiaires d'assurance (norme simplifiée n° 56) : https ://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000027837528.

18. Article 35, 4. du Règlement (UE) 2016/679 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 (règlement général sur la protection des données) : http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR.