CHRONIQUE

NOUVEAUX MOYENS DE PAIEMENT, BANQUE DIGITALE ET PROTECTION DES DONNÉES

PIERRE STORRER*
Avocat au Barreau de Paris
Kramer Levin Naftalis & Frankel LLP

MYRIAM ROUSSILLE
Agrégée des facultés de Droit
Professeur
Université du Mans
IRJS Sorbonne Affaires-Finance

Avec la collaboration **D'EMMANUEL JOUFFIN,** Docteur en droit, Responsable juridique de banque

LE RENDEZ-VOUS MANQUÉ ENTRE LA CJUE ET LE COMPTE DE PAIEMENT

Commentaire de Pierre Storrer

1. *Banque et Droit.* Fin 2016, *Banque et Droit* consacra un remarquable hors-série aux « nouveaux comptes ». Deux auteurs s'attachèrent notamment à sonder la notion de compte bancaire, pour l'un, de compte de paiement, pour l'autre ; compte de paiement, donc, faisant partie de ces nouveaux comptes, tel que créé par la première directive sur les services de paiement (DSP 1) et défini comme « *un compte qui est détenu au nom d'un ou de plusieurs utilisateurs de services de paiement et qui est utilisé aux fins de l'exécution d'opérations de paiement* » (art., 4, 14) ; définition reprise telle quelle par la DSP 2[1]. D'où il ressort que le compte de paiement, quelle que soit la qualité de l'établissement qui le tient (établissement de paiement, de monnaie électronique ou de crédit), s'appréhende immédiatement par sa fonction d'instrument de services de paiement[2] (eux-mêmes vecteurs de l'exécution d'opérations de paiement). D'où il advient, au contraire, que, tenu par un établissement de paiement (ou de monnaie électronique offrant des services de paiement), il se mue en « *pur compte de paiement* », selon l'heureuse expression de Myriam Roussille[3], en ce sens que lesdits établissements « *ne peuvent détenir que des comptes de paiement utilisés exclusivement pour des opérations de paiement* » (DSP 1, art. 16, 2)[4].

2. Depuis lors... Depuis 2007, depuis donc la DSP 1, on vivait assez bien sans s'interroger outre mesure sur la notion de compte de paiement, dont on remarquait que la tenue n'était pas constitutive d'un service de paiement *per se*, même si la réalité d'un tel compte est bien l'accessoire de l'exécution de la plupart des opérations de paiement[5]. Consensus régnait sur cette approche fonctionnelle, mêlée d'un peu d'institutionnel : « *Compte de paiement : compte détenu au nom d'une ou de plusieurs personnes, utilisé aux fins de l'exécution d'opérations de paiement. Les comptes de dépôt et les comptes courants ouverts auprès des établissements de crédit sont des comptes de paiement. Les comptes de paiement ouverts auprès des établissements de paiement présentent la caractéristique d'être exclusivement dédiés à l'exécution d'opérations de paiement ; il en résulte que l'établissement de paiement ne peut pas disposer des fonds pour son propre compte*[6]. »

1. Comp. CMF, art. L. 314-1, I : « *Est un compte de paiement, un compte détenu au nom d'une ou de plusieurs personnes, utilisé aux fins de l'exécution d'opérations de paiement.* »
2. Comme l'on peut lire que les comptes bancaires de dépôt ou les comptes courants sont des instruments de services bancaires : cf. Th. Bonneau, « La notion de compte bancaire », *Banque et Droit*, nov.-déc. 2016, hors-série « Nouveaux comptes & intérêts négatifs », p. 10.
3. Cf. M. Roussille, « La notion de compte de paiement », *Banque et Droit*, nov.-déc. 2016, hors-série « Nouveaux comptes & intérêts négatifs », p. 12.
4. Comp. CMF, art. L. 522-4, I : « *Les comptes ouverts par les établissements de paiement sont des comptes de paiement qui sont exclusivement utilisés pour des opérations de paiement. Cette destination exclusive doit être expressément prévue dans le contrat-cadre de services de paiement qui régit le compte.* »
5. Cf. G. Goffinet, « Le régime des comptes de paiement vu par le régulateur », *Banque et Droit*, nov.-déc. 2016, hors-série « Nouveaux comptes & intérêts négatifs », p. 22. Comp. L. de Pellegars, « Le compte de paiement », *Banque et Droit* n° 134, nov.-déc. 2010, p. 15.
6. E. Jouffin, O. Laplane et C. L'Hostis, « Transposition de la directive 2007/64/CE sur les services de paiement – Les nouvelles règles régissant la relation banque-client », hors-série *Banque et Droit*, déc. 2009, p. 12.

* Les propos de l'auteur n'engagent que celui-ci.

L'avènement de la directive Comptes de paiement[7] n'y changea rien, dont le « *dénuement notionnel* » est criant, car toute entière tournée vers « *la fourniture universelle de services de paiement* » (cons. 3) aux « *consommateurs* », dont le vocable remplace significativement l'expression DSP d'« *utilisateurs de services de paiement* ». Si bien que sa définition du compte de paiement veut dire à peu près la même chose que celle de la DSP 1 (ou 2) : « *un compte détenu au nom d'un ou de plusieurs consommateurs et servant à exécuter des opérations de paiement* » (art. 2,3). Or voilà que ce théâtre d'ombres ne résiste pas à la lumière crue portée sur le compte de paiement par la DSP 2. Désormais, en effet, les prestataires de services de paiement (PSP) se distribuent selon qu'ils gèrent des comptes de paiement (PSP dits « *gestionnaires de comptes* », qui fournissent et gèrent un compte de paiement pour un payeur) ou offrent des services d'accès à des comptes en ligne qu'ils ne tiennent pas (prestataires de services d'initiation de paiement et prestataires de services d'information sur les comptes). Si bien qu'il devient urgent de préciser les contours de la notion de compte de paiement afin de déterminer ceux auxquels les nouveaux prestataires peuvent avoir accès, ou pas. On se souvient à cet égard du blocage de la Commission mixte paritaire lors de l'examen du projet de loi de ratification de l'ordonnance de transposition de la DSP 2, sachant que – les uns et les autres au demeurant pour de bonnes raisons – les sénateurs entendaient ouvrir l'accès aux comptes sur livret, à terme, d'épargne, etc., cependant que les députés s'y opposaient en faisant valoir la lettre de la directive, qui ne pouvait porter que sur les services, opérations et comptes de paiement[8]. De là l'intérêt – à la hauteur de notre déception – de prendre connaissance du premier arrêt de la Cour de justice de l'Union européenne rendu à propos de la notion de compte de paiement (CJUE, 4 oct. 2018, aff. C-191/17, *Bundeskammer für Arbeiter und Angestellte c/ ING-DibBa Direktbank Austria Niederlassung der ING-DiBa AG*[9]).

3. Réponse à la question préjudicielle posée. La question préjudicielle portait sur le point de savoir si un type spécifique de comptes bancaires : en l'espèce des comptes d'épargne en ligne disponibles à vue (en ce sens que « *les clients peuvent disposer des sommes versées sur ces comptes à tout moment sans qu'il en résulte une répercussion négative sur les intérêts produits* »[10]), au titre desquels le consommateur dispose d'un accès illimité aux fonds déposés, mais ne peut effectuer ou recevoir des virements vers ou de l'extérieur que par l'intermédiaire d'autres comptes appelés « *comptes de référence* », relèvent ou non de la notion de « *compte de paiement* » telle que donnée par l'article 4, 14, de la DSP 1 (ou 4, 12 de la DSP 2, mais qui n'était pas applicable au cas présent). Après que l'avocat général, M. Evgeni Tanchev, a donné son point de vue avant même de l'argumenter – ce qui est assez rare : « *[...] je suis parvenu à la conclusion que le compte épargne direct en ligne concerné ne peut pas être considéré comme relevant de la notion de "compte de paiement"* »[11], la Cour de justice apporte elle-même une réponse négative, selon laquelle l'article 4, 14 précité « *doit être interprété en ce sens que ne relève pas de la notion de "compte de paiement" un compte d'épargne qui permet de disposer de sommes déposées à vue et à partir duquel des opérations de versement et de retrait ne peuvent être effectuées que par l'intermédiaire d'un compte courant* »[12]. La solution est sans doute pertinente, mais pas sa motivation. À telle enseigne que nous avons rarement vu conclusions et décision aussi courtes, contrastant singulièrement avec le style auquel nous ont habitués la CJUE et ses avocats généraux.

4. Critique. Le *hic*, en effet, est que, faute de trouver matière dans la DSP 1, M. l'avocat général, puis l'arrêt lui-même, fondent leur interprétation sur la directive Comptes de paiement (bien que, relève la Cour, elle « *ne soit pas directement applicable au litige au principal* »[13]), dont on a dit plus haut qu'elle était vide de toute notion, en particulier de toute notion de compte de paiement. Sont donc convoqués et le considérant 12 de la directive de 2014 et son article 1er, 6, desquels la juridiction européenne tire que « *la possibilité d'effectuer, à partir d'un compte, des opérations de paiement en faveur d'un tiers ou de bénéficier de telles opérations effectuées par un tiers est un élément constitutif de la notion de "compte de paiement"* »[14]. Sauf que le considérant 12 ne dit pas cela, mais plein d'autres choses : qu'une partie des dispositions de la directive est applicable à tous les PSP (comparabilité des frais et changement de compte), tandis que l'autre (accès aux comptes assortis de prestations de base) ne s'applique qu'aux établissements de crédit ; ou que si, par exemple, les comptes d'épargne, les comptes liés à une carte de crédit, les comptes de monnaie électronique, etc., devraient en principe être exclus du champ d'application du texte, ils en relèveraient toutefois s'ils devaient être utilisés pour « *exécuter des opérations de paiement quotidiennes* » ; ou, encore, que les comptes détenus par des entreprises (mêmes petites ou microentreprises) n'en relèvent pas. Or ce dernier exemple est significatif : les comptes des entreprises n'échappent pas au champ d'application de la directive Comptes de paiement parce qu'ils ne sont pas des comptes de paiement, mais tout simplement parce que ce texte ne s'applique qu'aux comptes détenus par des « *consommateurs* », ce qu'énonce parfaitement son article 1er, 6 : « *La présente directive s'applique aux comptes de paiement permettant aux consommateurs d'effectuer au moins les opérations suivantes : a) verser des fonds sur un compte de paiement ; b) retirer des espèces d'un compte de paiement ; c) exécuter des opérations de paiement, y compris des virements, en faveur d'un tiers et être les bénéficiaires de telles opérations effectuées par un tiers* ». N'est-il pas contestable d'inférer de cette délimitation du champ d'application

7. Dir. 2014/92/UE, 23 juill. 2014, sur la comparabilité des frais liés aux comptes de paiement, le changement de compte de paiement et l'accès à un compte de paiement assorti de prestations de base.

8. Cf. P. Storrer, « Sur la loi de ratification de l'ordonnance de transposition de la DSP 2 », *Revue Banque* n° 824, oct. 2018, p. 92.

9. Nous remercions Myriam Roussille d'avoir porté cet arrêt à notre connaissance, ainsi qu'un premier commentaire qu'elle en a fait : « Comptes de paiement : et si la CJUE contribuait à clarifier les règles du jeu ? », *Bulletin Dictionnaire européen de droit des affaires* n° 361, Éditions législatives, p. 13.

10. Point 13 de l'arrêt.

11. Point 23 des conclusions.

12. Point 34 de l'arrêt.

13. Point 26 de l'arrêt.

14. Point 31 de l'arrêt.

de la directive que les comptes de paiement devraient au minimum permettre de telles actions pour pouvoir être qualifiés tels ? Ne l'est-il pas davantage encore lorsque le dernier alinéa dudit point 6 dispose : « *Les États membres peuvent décider d'appliquer la totalité ou une partie de la présente directive à des comptes de paiement autres que ceux visés au premier alinéa* » ? C'est bien que la notion de compte de paiement n'est pas qualifiée, ou disqualifiée, selon que les régimes prévus par la directive (comparabilité des frais liés aux comptes de paiement, changement de compte de paiement et accès à un compte de paiement assorti de prestations de base) s'appliquent ou non ; c'est, au contraire, le seul champ d'application de chacun de ces régimes qui est ordonné par ce texte[15].

5. Espoir déçu. Cela aurait pu être un grand arrêt ; cela aurait même dû l'être, mais il ne fallait pas, pour cela, faire parler la directive 2014/92/UE, qui n'a rien à voir avec la notion de compte de paiement, comme son l'intitulé au demeurant le laisse entendre. L'avocat général Tanchev a fait fausse route en cherchant dans les « *dispositions connexes* » de la DSP 1 (en vérité, essentiellement la directive Compte de paiement) l'élément qu'il juge déterminant en ce qui concerne la qualification de compte de paiement : « *le paiement en faveur d'un tiers* »[16]. Non pas, d'ailleurs, que cela ne soit pas pertinent – comme il serait intéressant de creuser ce que l'on appelle parfois compte « interne » ou « technique »[17], privés de cette faculté d'extériorisation qui caractériserait, peut-être, le compte de paiement, voire tous les comptes bancaires –, comme l'est sans doute l'analyse en termes de « fonctions » de paiement exposée au considérant 12 de la directive. Mais si ces éléments ne se trouvent pas dans la DSP (1 ou 2), il est plus que contestable d'aller les chercher ailleurs. En particulier, la directive Comptes de paiement ne peut venir au secours des directives Services de paiement. Leur silence, pour l'heure, s'impose. ■

Achevé de rédiger le 19 novembre 2018.

15. Ce pourquoi nous apparaît comme un contresens majeur ce passage, en particulier, des conclusions de M. l'avocat général : « *Cela est concrétisé à l'article 1er, point 6, de la directive 2014/92, qui indique explicitement que les trois exigences minimales applicables aux comptes de paiement relevant du champ d'application de cette directive sont la faculté de verser des fonds sur un compte de paiement, de retirer des espèces d'un tel compte et d'"exécuter des opérations de paiement, y compris des virements, en faveur d'un tiers et être les bénéficiaires de telles opérations effectuées par un tiers".* »

16. Point 46 des conclusions.

17. Cf. Th. Bonneau, *op. cit.*, p. 8.

■ RGPD ET ANALYSE D'IMPACT : LA CNIL FIXE SA DOCTRINE

Commentaire d'Emmanuel Jouffin

La CNIL poursuit son œuvre pédagogique en matière d'analyse d'impact s'agissant des traitements de données personnelles les plus risqués. Après avoir diffusé en février 2018 un document intitulé « *Analyse d'impact relative à la protection des données – Privacy Impact Assessment (PIA) – Les bases de connaissances* »[1], celle vient de publier deux délibérations sur ce sujet.

Tout d'abord, par une délibération n° 2018-326 du 11 octobre 2018 (JO du 6 novembre), la CNIL fixe des principes généraux sur le périmètre des analyses d'impact relatives à la protection des données (AIPD), sur le mode opératoire et le périmètre de l'obligation de porter à sa connaissance les résultats d'une AIPD. Par une seconde délibération, n° 2018-327 du même jour[2], la CNIL livre une liste de traitements devant nécessairement donner lieu à une analyse d'impact relative à la vie privée (AIPD).

I. GÉNÉRALITÉS

La délibération n° 2018-326 précise le périmètre de l'obligation de conduire une analyse d'impact, les conditions de réalisation et indique que des référentiels sectoriels sont à venir et que, certains d'entre eux, produiront des effets juridiques, exonérant de la réalisation d'AIPD « *les responsables de traitement qui s'y conformeraient strictement* ».

Par ailleurs, cette délibération rappelle les types de traitement soumis obligatoirement à analyse d'impact au sens de l'article 35-1 du RGPD (profilage automatisé, traitement à grande échelle de données sensibles et vidéoprotection dans les zones accessibles au public), ainsi que les 9 critères retenus par le G29[3] pour déterminer si un traitement est susceptible d'engendrer un risque élevé pour les personnes (cf. tableau 1)

Pour le G29, c'est lorsque deux de ces critères sont remplis qu'une analyse d'impact doit être menée, cependant, un seul peut parfois suffire au regard du traitement envisagé. Il sera cependant possible de s'écarter de la recommandation ci-dessus dans certains cas de figure si le responsable de traitement prouve, de manière documentée que, même en présence de deux des critères mentionnés ci-dessus, il n'existe pas de « risque élevé »[4].

1. https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf.

2. Délibération n° 2018-327 du 11 octobre 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.

3. Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « *susceptible d'engendrer un risque élevé* » aux fins du règlement (UE) 2016/679. Adoptées le 4 avril 2017 modifiées et adoptées en dernier lieu le 4 octobre 2017.

4. Lignes directrices, p. 13.

Tableau 1. Les critères retenus par le G29 pour déterminer si un traitement est susceptible d'engendrer un risque élevé pour les personnes

Types de données	Cas d'application
Données traitées à grande échelle	Traitements de données de type *Big Data*
Données sensibles (origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques ou de santé, données biométriques et données concernant la vie ou l'orientation sexuelle)	Notamment, questionnaires de santé lors de l'examen d'un dossier de crédit
Données à caractère hautement personnel (données relatives à des communications électroniques, données de localisation, données financières, etc.)	Notamment données des cartes bancaires (cf. Délibération CNIL 2018-303 du 6 septembre 2018 – Traitement des données cartes bancaires en matière de vente à distance)
Données concernant des personnes vulnérables (patients, personnes âgées, enfants, etc.)	Notamment dossiers concernant des majeurs protégés et mineurs
Croisement ou combinaison de données	Notamment traitements de données de type *Big Data*, profilage
Prise de décision automatisée avec un effet juridique ou similaire	Traitements de profilage
Surveillance systématique de personnes	Notamment la vidéosurveillance, la biométrie
Traitement pouvant exclure du bénéfice d'un droit, d'un service ou d'un contrat	Traitements de profilage
Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles	Notamment développement *Blockchain* au regard de l'exercice des droits des personnes concernées, développement d'applications ayant recours à l'IA

Cet article 35-1 prévoit également que le responsable doit effectuer une AIPD lorsqu'un traitement est susceptible d'engendrer « *un risque élevé pour les droits et libertés des personnes physiques* ». On soulignera que le considérant 75 du RGPD vise expressément les cas de profilage parmi les types de traitements pour lesquels une analyse d'impact peut être exigée. La délibération précise que les traitements régulièrement mis en œuvre avant le 25 mai 2018 n'ont pas à faire l'objet d'une analyse d'impact dans un délai de 3 ans, à moins d'une modification substantielle, sans toutefois préciser ce qu'est une modification substantielle. Une décision de transfert de données hors UE, ou bien une modification de la finalité, ou bien encore l'apparition de l'un des neuf critères du G29 peuvent constituer des indices pertinents.

Concernant les conditions de réalisation de l'analyse d'impact, la CNIL exige qu'elle soit menée avant la mise en œuvre du traitement et qu'elle soit revue régulièrement (au plus tard tous les 3 ans). Cette analyse d'impact doit au moins être faite en présence du DPO, du RSSI, des sous-traitants concernés, de représentants des personnes concernées et du maître d'ouvrage/maître d'œuvre. Chaque étape doit être documentée et, en cas de risque résiduel, la CNIL devra être saisie.

La Délibération établit une liste des traitements pour lesquels une analyse d'impact est obligatoire, notamment pour le profilage à des fins de gestion RH, la gestion des alertes et signalements en matière professionnelle ou encore la localisation à large échelle. Cette liste sera régulièrement mise à jour par la CNIL.

Les AIPD pourront, en application des articles 58 du RGPD et 44 de la loi du 6 janvier 1978, être demandées aux responsables de traitement, notamment dans le cadre de l'instruction des plaintes dont elle serait saisie ou dans le cadre du contrôle de la mise en œuvre des traitements.

Lorsqu'il ressort d'une AIPD que le responsable du traitement est d'avis que le risque ne peut être atténué par des moyens raisonnables compte tenu des techniques disponibles et des coûts de mise en œuvre, il y a lieu de consulter l'autorité de contrôle avant le début des opérations de traitement[5].

II. DÉLIBÉRATION N° 2018-326 – LISTE CNIL DES TRAITEMENTS SOUMIS À AIPD

Dans la « *liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise* » publiée par la CNIL en marge de la sa délibération du 11 octobre 2018, certains concernent plus particulièrement les activités bancaires. Les principaux sont présentés dans le Tableau 2.

5. Considérant 94 du RGPD.

Tableau 2. Opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise

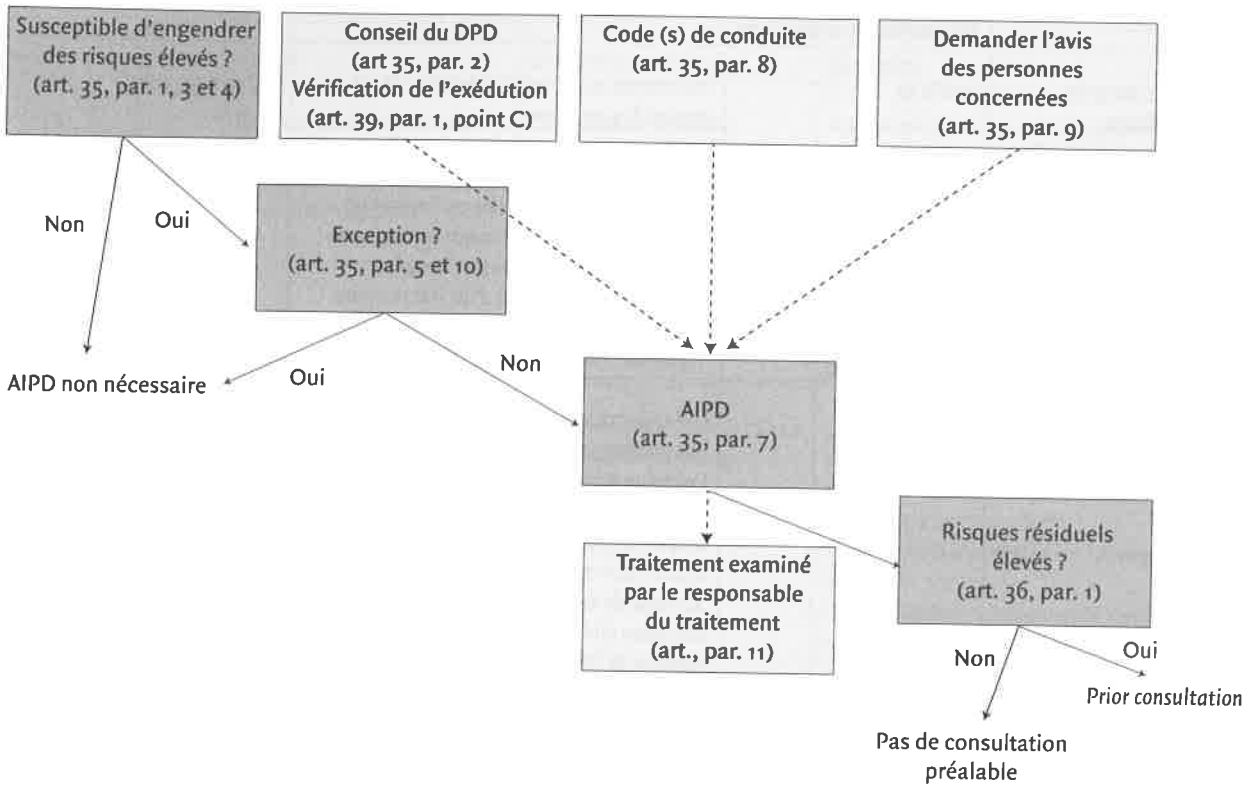
Domaines	Nature	Critères issus du G29	Exemples
RH	Traitements établissant des profils de personnes physiques à des fins de gestion des ressources humaines	Évaluation ou notation Personnes dites « vulnérables »	Traitement de détection et de gestion de « hauts potentiels » Traitement visant à faciliter le recrutement, notamment grâce à un algorithme de sélection Traitement visant à proposer des actions de formations personnalisées grâce à un algorithme Traitement visant détecter et à prévenir les départs de salariés sur la base de corrélations établies entre divers facteurs
RH – Salle de marchés – Activités de guichet – transport de fonds	Traitements ayant pour finalité de surveiller de manière constante l'activité des employés concernés	Personnes dites « vulnérables » Surveillance systématique	Dispositif de cyber surveillance tels que ceux procédant à une analyse des flux de courriels sortants afin de détecter d'éventuelles fuites d'information (dispositifs dits de *Data Loss Prevention*) Vidéosurveillance portant sur les employés manipulant des fonds Vidéosurveillance d'un entrepôt stockant des biens de valeur au sein duquel travaillent des manutentionnaires
RH – Dispositif d'alerte déontologique	Traitements ayant pour finalité la gestion des alertes et des signalements en matière sociale et sanitaire		Cf. *infra* « alertes professionnelles »
Banque toutes activités dont crédit, lutte anti-fraude et anti-blanchiment	Traitements impliquant le profilage des personnes pouvant aboutir à leur exclusion du bénéfice d'un contrat ou à la suspension voire à la rupture de celui-ci	Évaluation ou notation Croisement ou combinaison d'ensembles de données	Traitement établissant un score pour l'octroi de crédit Traitement reposant sur une analyse comportementale visant à détecter des comportements « interdits » sur un réseau social Traitement de lutte contre la fraude aux moyens de paiement
Fichiers d'incidents Banque de France - Assurance	Traitements mutualisés de manquements contractuels constatés, susceptibles d'aboutir à une décision d'exclusion ou de suspension du bénéfice d'un contrat	Croisement ou combinaison d'ensembles de données Prise de décision automatisée avec effet juridique ou similaire significatif	Traitement recensant les impayés et souscriptions irrégulières partagé par un secteur d'activité Traitement des résiliations automobiles permettant aux sociétés d'assurances de vérifier les antécédents d'un futur assuré lors de la demande de souscription d'un contrat d'assurance automobile
Banque toutes activités	Traitements de profilage faisant appel à des données provenant de sources externes	Évaluation ou notation Croisement ou combinaison d'ensembles de données Usage innovant ou application de nouvelles solutions technologiques Collecte de données sensibles	Combinaison de données opérée par des courtiers en données (data brokers) Traitement visant à personnaliser les publicités en ligne
Alertes professionnelles Point d'attention particulière dans le cadre de la mise en place du dispositif Sapin II à l'égard des lanceurs d'alerte	Traitements ayant pour finalité la gestion des alertes et des signalements en matière professionnelle	Personnes dites « vulnérables » Évaluation ou notation Collecte de données sensibles	Dispositif de recueil d'alertes professionnelles pour les organismes privés ou publics concernés Dispositif de recueil de signalements concernant des faits de trafic d'influence ou de corruption commis au sein de l'organisme Dispositif d'alerte mis en œuvre dans le cadre du devoir de vigilance.

Cas particulier du profilage

Type de profilage concerné	Article visé pour la détermination du profilage	Principes du traitement	AIPD obligatoire
Profilage impliquant une prise de décision exclusivement automatisée et produisant des effets juridiques (critères cumulatifs)	Article 22	Traitements par principe interdits – Droit attaché à la personne Exceptions – Nécessaire à la formation ou l'exécution d'un contrat à la condition que soient prises des mesures appropriées (art. 22-a)[6] – ou conformité au droit d'un État membre (art. 22b) – consentement explicite (art. 22 - c)	Oui (art. 35, 3 a)
Profilage impliquant une prise de décision non exclusivement automatisée produisant des effets juridiques	Article 35, § 3 a)	Licéité du traitement (art. 6) Consentement Exécution d'un contrat ou de mesures précontractuelles Respect d'une obligation légale s'imposant au responsable du traitement Sauvegarde des intérêts vitaux Exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique Intérêts légitimes poursuivis par le responsable du traitement ou par un tiers[7]	Oui (art. 35, 3 a)
Profilage sans prise de décision, à des fins de prospection	Article 21, § 2	*Idem* ci-dessus	Non – la recommandation vise les traitements impliquant le profilage des personnes pouvant aboutir à une exclusion ou à une suspension ou rupture d'un contrat – L'absence de prise de décision exclut un risque et donc la nécessité d'une AIPD
Profilage à des fins d'analyse ou d'évaluation sans finalité de prospection et sans prise de décision	Article 4	*Idem* ci-dessus	Non – *Idem* ci-dessus
Types de données supports de profilage	Article 22-4 et 9-1[8]	Exceptions : art. 9-2 a et g[9]	Oui (art. 35, 3 a)

6. Pour les 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* » (art. 22-3).
7. Le responsable doit être en mesure de prouver que le profilage est nécessaire, en tenant compte du fait qu'une méthode moins envahissante pourrait être adoptée. Si d'autres moyens moins attentatoires pour atteindre le même but existent, le profilage ne serait pas « nécessaire ».
8. « *Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.* »
9. Consentement de la personne et nécessité pour des motifs d'intérêt public important dans le respect de la proportion à l'objectif poursuivi, et adoption de « *mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée* ».

Schéma décisionnaire d'une AIPD



Source : Lignes directrices du G29.