LES MATINALES PDGB

-

ACTUALITÉS DU DROIT DE LA PROTECTION DES DONNEES A CARACTÈRE PERSONNEL

Hélène Lebon
Avocat Associé

Sandra Tubert
Avocat

7 juillet 2015

SOMMAIRE

I. **Opérations de prospection commerciale:** analyse des dernières sanctions prononcées par la CNIL et des récentes décisions du Conseil d'Etat

II. **Mise en place de listes d'exclusion et traitement de données relatives à des infractions:** analyse de la dernière décision du Conseil d'Etat

III. **La prise en compte des risques de sanctions en recourant à des prestataires:** analyse des décisions de la CNIL et du Conseil d'Etat prononçant des sanctions à l'encontre d'entreprises pour des manquements à la loi I&L commis par les sous-traitants

OPÉRATIONS DE PROSPECTION COMMERCIALE

Analyse des dernières sanctions prononcées par la CNIL et des récentes décisions du Conseil d'Etat

RISQUES ET SANCTIONS

- **Article L.34-5 CPCE**: amende administrative 3 000 € et 15 000 € pour personnes morales

- **Article R.10-1 CPCE**: amende pour chaque correspondance ou appel 750€ et 3 750€ pour personnes morales

- **Article L. 121-34-1-1 Code consommation** (par voie téléphonique uniquement): 15 000 € et 75 000€ pour personnes morales

- **Articles 226-18 et 226-18-1 Code Pénal** (collecte déloyale et non respect du droit d'opposition): 5 ans d'emprisonnement et 300 000€ d'amende (jusqu'à 1 500 000€ pour personnes morales)

- Contrôles de la DGCCRF

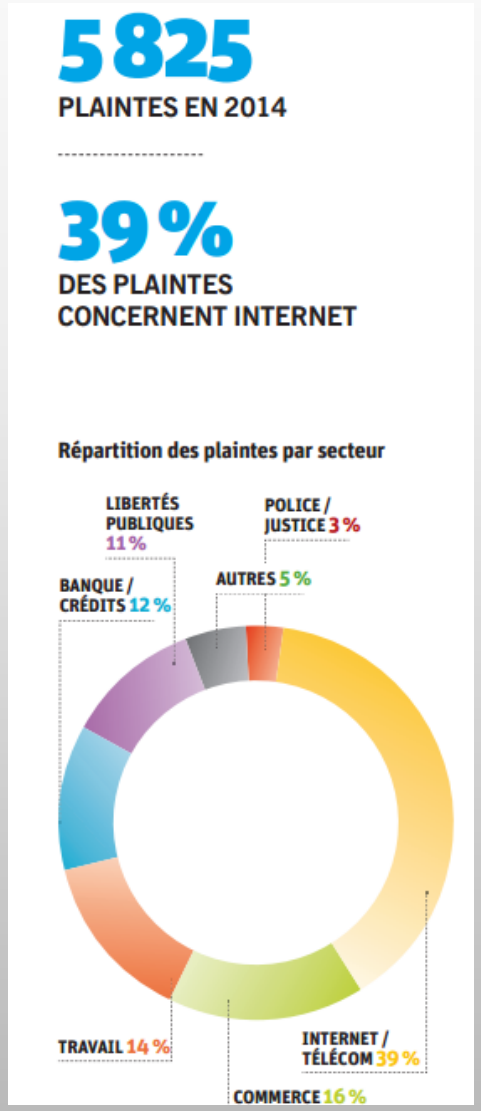
RISQUES ET SANCTIONS

- **Art. 45 s. loi I&L:**

  - ✓ Mise en Demeure
  - ✓ Avertissement
  - ✓ Injonction de cesser le traitement
  - ✓ Sanction pécuniaire : 150 000 € (et 300 000 € en cas de récidive)

- Bilan 2014 de l'activité de la CNIL: **une activité répressive en hausse**

RISQUES ET SANCTIONS



- **Prospection Commerciale:**
  - l'un des principaux motifs de plaintes devant la CNIL (16%),
  - l'un des focus de la CNIL.

LE CONTRÔLE DU JUGE SUR LA CNIL

- **Sur les dossiers perdus: CE 10ème ss-section, 7 janvier 2015, N°372328**
  - Demande de condamnation CNIL au versement de 30 000 euros pour la perte du dossier de plainte
  - Incompétence du CE ➔ Tribunal Administratif

- **Sur la gestion des plaintes abusives: CE 10ème et 9ème SSR, 10 avril 2015, N°376575**
  - La CNIL peut rejeter les plaintes dont elle est saisie lorsqu'elles présentent un caractère abusif
  - Mais elle ne peut pas rejeter des plaintes sans examen préalable de chacune d'elles

LES DÉCISIONS RÉCENTES

- **CE 23 mars 2015, 10ème/9ème SSR**
  - Prospection par SMS – information/cst des personnes – cessions de données
- **CE 11 mars 2015, 10ème/9ème, SSR TUTO4PC**
  - Prospection par mail – information/cst des personnes
- **CNIL 1er juin 2015, Prisma Media**
  - Inscription aux newsletters du Groupe (cst) – durée de conservation

RÉGIME JURIDIQUE APPLICABLE

- Les textes:
  - Art. 38 loi I&L
  - Art. L. 34-5 du CPCE et L. 121-34 CConso
- La règle applicable dépend du canal de prospection (postale, téléphonique ou électronique)
- Sanctions pénales et/ou administratives importantes

RÉGIME JURIDIQUE APPLICABLE

PROSPECTION COMMERCIALE PAR VOIE POSTALE ET TELEPHONIQUE (hors automates d'appels) :

- Principe de l'« Opt-out»

- Art. 38 al 2 loi I&L:

  La personne concernée *"a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur"*

- Article 96 Décret n°2005-1309: *"l'interessé est mis en mesure d'exprimer son choix avant la validation définitive de ses réponses."*

- Loi Hamon: création Article L.121-34 Cconso → liste d'opposition au démarchage téléphonique

RÉGIME JURIDIQUE APPLICABLE

PROSPECTION COMMERCIALE PAR VOIE ELECTRONIQUE (Article L34-5 CPCE) DANS LE CONTEXTE B TO C

- La prospection commerciale par voie électronique recoupe la prospection par email, SMS, MMS…
- Le consentement préalable de la personne concernée (opt-in) : **libre, spécifique et informé**
- Interdiction de dissimuler l'identité de l'expéditeur ou l'objet de la communication

RÉGIME JURIDIQUE APPLICABLE

PROSPECTION COMMERCIALE PAR VOIE ELECTRONIQUE (Article L34-5 CPCE) DANS LE CONTEXTE B TO C

- Exception au principe du consentement préalable (opt-out) si les conditions suivantes sont réunies:

  - ✓ Coordonnées recueillies directement auprès du destinataire
  - ✓ Dans le respect de la loi Informatique et libertés
  - ✓ À l'occasion d'une vente ou d'une prestation de service
  - ✓ Prospection concernant des produits ou services analogues
  - ✓ Fournis par la même personne physique ou morale

La constante : prévoir un droit d'opposition sur le courrier électronique

RÉGIME JURIDIQUE APPLICABLE

PROSPECTION COMMERCIALE PAR VOIE ELECTRONIQUE (Article L34-5 CPCE) DANS LE CONTEXTE B TO B

- Encadrée par l'article L34-5 CPCE
- Pratique et recommandation de la CNIL: opt-out
- Modification de l'article L34-5 par l'ordonnance du 24 aout 2011: l'opt-in désormais requis dans le contexte B to B?

« Est interdite la prospection directe au moyen de systèmes automatisés d'appel ou de communication, d'un télécopieur ou de courriers électroniques utilisant les coordonnées d'une personne physique, ***abonné ou utilisateur,*** *qui n'a pas exprimé préalablement son consentement à recevoir des prospections directes par ce moyen ».*

LES DIFFÉRENTS CANAUX

- PROSPECTION PAR VOIE POSTALE : **OPT-OUT**
- PROSPECTION TELEPHONIQUE SANS AUTOMATE D'APPELS : **OPT-OUT**
- PROSPECTION TELEPHONIQUE AVEC AUTOMATE D'APPELS : **OPT-IN (PAS D'EXCEPTION)**
- PROSPECTION PAR TELECOPIE : **OPT-IN (PAS D'EXCEPTION)**
- PROSPECTION PAR COURRIER ELECTRONIQUE (E-MAIL, SMS, MMS) : **OPT-IN**

EXCEPTION : OPT-OUT SI CONDITIONS SUIVANTES REUNIES :

- ✓ coordonnées recueillies directement auprès du destinataire du message;
- ✓ à l'occasion d'une vente ou d'une prestation de services ;
- ✓ en ayant respecté les principes de la loi informatique et libertés ;
- ✓ pour de la prospection concernant des produits ou services analogues ;
- ✓ fournis par la même personne physique ou morale.

RAPPEL SUR LE RÉGIME JURIDIQUE APPLICABLE

CONSTANTES POUR TOUTE FORME DE PROSPECTION:

- Toujours faire figurer le **droit d'opposition** → coordonnées valables pour transmettre une demande pour que ces communications cessent sans frais

- Interdiction de dissimuler l'identité de la personne et/ou de mentionner un objet sans rapport avec la prestation ou le service proposé

- Pour la CNIL, **l'acceptation de CGV, mentions légales ou les cases pré-cochées ne sont pas considérées comme des modalités valables de recueil du consentement**

PROSPECTION PAR SMS

- Délibération n° 2011-384 du 12 janvier 2012 de la CNIL prononçant une **sanction de 20 000€** à l'encontre du Groupe DSE France

- **Manquements reprochés:**
  - Ne pas avoir respecté l'article L. 34-5 CPCE (opt-in) : collecte indirecte de données → la société aurait dû veiller à **acheter un fichier « opt-inisé** »;
  - Ne pas avoir informé les personnes conformément à l'article 32 loi I&L: collecte indirecte → la société aurait dû **insérer mention d'information complète dans le SMS envoyé;**
  - Ne pas avoir mis à disposition **un droit d'opposition gratuit et efficace.**

PROSPECTION PAR SMS

- Conseil d'Etat, 23 mars 2015, 10ème/9èmeSSR, n°357556: **confirme la délibération de la CNIL**

- Consentement préalable à recevoir de la prospection commerciale par SMS est nécessaire

- Acquisition fichiers clients = collecte indirecte de données: les **personnes doivent être correctement informées** conformément à l'article 32 loi I&L → **refus de prise en compte des dérogations/exceptions (impossibilité d'informer ou efforts disproportionnés)**

- Droit d'opposition: envoi d'un SMS payant ou d'un appel téléphonique payant n'est pas conforme aux dispositions de l'article 38 loi I&L

PROSPECTION PAR SMS

CE QU'IL FAUT EN RETENIR:

- Veiller à **acquérir des fichiers dits « opt-inisé »** → La responsabilité pèse sur celui qui réalise l'opération de prospection;

  → Insérer une garantie dans le contrat d'achat fichiers client ou licence utilisation BDD

- En cas de **collecte indirecte** de données (ex: achat fichiers clients) → insérer une **mention d'information complète des personnes** lors de l'envoi de la prospection

- Mettre en place un **droit d'opposition GRATUIT** peu importe sa forme (n° vert, SMS gratuit, lien hypertexte) **et EFFECTIF** (veiller à ce que votre BDD ou CRM gère bien les opt-in et opt-out)

CONSENTEMENT PAR ACCEPTATION DE CGU

- Conseil d'Etat, 11 mars 2015, 10ème/9ème SSR n°368624, TUTO4PC : décision rendue à l'encontre d'une **mise en demeure de la CNIL**

- TUTO4PC propose des logiciels gratuits → l'acceptation des CGU entraîne l'installation d'un moteur de recherche, l'envoi de publicités adaptées en fonction du suivi des connexions de l'utilisateur et la cession de données personnelles à des tiers.

- MED CNIL:
  - recueillir le consentement spécifique des personnes pour de la prospection;
  - cesser l'installation de cookies sans accord préalable;
  - cesser la collecte d'adresses IP et identifiants uniques à l'insu des personnes.

CONSENTEMENT PAR ACCEPTATION DE CGU

- Conseil d'Etat, 11 mars 2015, TUTO4PC:

« Considérant, en deuxième lieu, que le consentement spécifique exigé par les dispositions de l'article L. 34-5 du code des postes et communications électroniques ne peut résulter que du ***consentement exprès de l'utilisateur, donné en toute connaissance de cause et après une information adéquate sur l'usage qui sera fait de ses données personnelles*** *; qu'alors même que, comme le soutient la société, l'information serait suffisante et les conditions générales d'utilisation claires et explicites, le* ***consentement donné à ces dernières pour l'ensemble des finalités d'un traitement, dont l'usage des données personnelles de l'utilisateur, ne saurait être regardé comme valant consentement spécifique****, au sens et pour l'application de l'article L. 34-5 précité »*

CONSENTEMENT PAR ACCEPTATION DE CGU

Pour le Conseil d'Etat :

- consentement via l'acceptation de CGU: pas conforme aux conditions de l'article L. 34-5 CPCE : une manifestation de volonté libre, **spécifique** et informée

- Modalités d'acceptation insuffisantes:
  - Formulaire de collecte précisant *« qu'en acceptant les CGU, vous consentez à ce que ces informations puisse faire l'objet d'une exploitation commerciale, d'une communication à des tiers ou d'une cession »*
  - les CGU étaient acceptées 3 fois

- rejoint la CNIL dans **l'appréciation du caractère spécifique et exprès du consentement → un consentement exprimé sur ce point et lui seul.**

CONSENTEMENT PAR ACCEPTATION DE CGU

Pour le Conseil d'Etat :

- La personne qui a recueilli et cédé les données doit *« prendre toutes les mesures pour que les données ne soient plus utilisées par les cessionnaires »,* c'est à dire, les **informer qu'elle n'a pas respecté les obligations en matière de prospection** pour que les cessionnaires puissent:

  - se conformer eux-mêmes à la loi en recueillant le consentement spécifique, ou
  - suspendre l'utilisation des données en attendant une régularisation du cédant, ou
  - cesser d'utiliser les données

CONSENTEMENT PAR ACCEPTATION DE CGU

CE QU'IL FAUT EN RETENIR:

- **Prévoir une/des case(s) « d'opt-in »** lorsqu'une utilisation à des fins commerciales des données est envisagée

- Ne **pas diluer l'information** quant à l'utilisation des données à des fins de prospection commerciale dans des CGU/CGV/mentions légales

- **Tenir les cessionnaires informés** de l'opposition des personnes à la réception de prospection commerciale, mais également d'une absence de respect des dispositions applicables en matière de prospection commerciale

CESSION DE DONNEES

CE QU'IL FAUT RETENIR DE CES DECISIONS:

- Le cessionnaire doit vérifier que le cédant a recueilli un consentement conforme à la loi
- La CNIL peut mettre le cédant en demeure d'informer les cessionnaires qu'il n'a pas respecté les exigences légales
- Le cessionnaire doit ensuite prendre les actions nécessaires

COLLECTE DE DONNÉES & ENVOI DE NEWSLETTERS

- Délibération n°2015-155 du 1er juin 2015 **sanction de 15 000€**

- **Manquements reprochés:**

  - Non-respect art. L34-5 CPCE: case recueillant le consentement doit **lister l'intégralité des newsletters qui seront envoyées à l'internaute**

  - Non-respect art. 32 I&L: mention d'information doit être complète et **préciser notamment le droit d'opposition au traitement**

COLLECTE DE DONNÉES & ENVOI DE NEWSLETTERS

- **Manquements reprochés:**

  - Non-respect de la durée de conservation posée par la NS 48 et du point de départ de ce délai (violation art. 6 5°)

  - **Pour la société**: durée de conservation 760 jours (2 ans et 30 jours) avec comme point de départ l'ouverture de la newsletter ou le clic proposé dans la newsletter par les personnes concernée

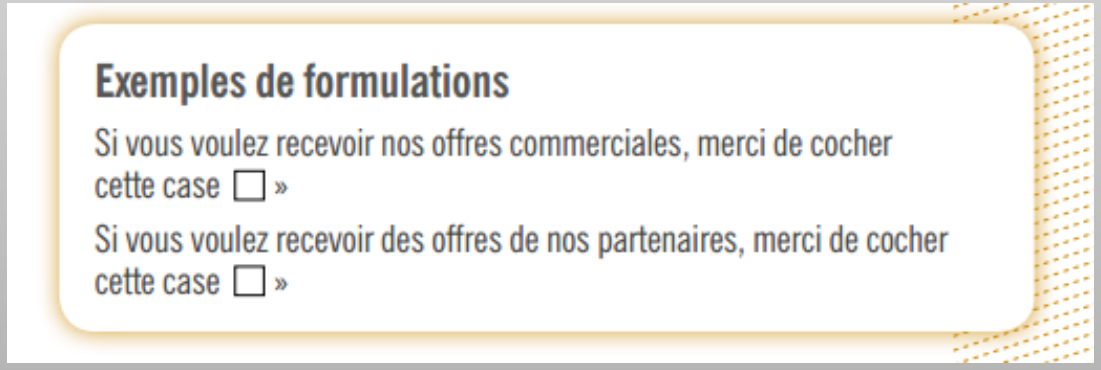
  - **Pour la CNIL**: 3 ans à compter de la collecte ou du dernier contact (NS 48):
    - Le clic sur le lien hypertexte peut constituer un contact au sens NS48
    - L'ouverture de la newsletter n'est pas valable comme contact au sens NS48

COLLECTE DE DONNÉES & ENVOI DE NEWSLETTERS

CE QU'IL FAUT EN RETENIR:

- *« □ oui, je souhaite recevoir les newsletters du Groupe Prisma Media »* ne constitue pas un consentement libre, spécifique et informé à recevoir les newsletters pour les autres titres du groupe, ni pour des biens et services de tiers → pour la CNIL il faut **donner une liste exhaustive des newsletters auxquelles l'internaute souscrit quand il coche la case**.

- **Appréciation stricte et extensive**, surprenante si l'on prend en compte les modèles « d'opt-in » de la CNIL:



COLLECTE DE DONNÉES & ENVOI DE NEWSLETTERS

CE QU'IL FAUT EN RETENIR:

- La **mention relative au droit d'opposition doit figurer sur le formulaire de collecte des données** et pas sur un autre support (art. 32)

- Caractère non obligatoire de la collecte des données et la présence d'un "opt-in" sont sans incidence sur l'obligation d'insérer une mention sur le droit d'opposition (peut être exercé *a posteriori*)

COLLECTE DE DONNÉES & ENVOI DE NEWSLETTERS

CE QU'IL FAUT EN RETENIR:

- **Attention au recours aux normes simplifiées**: problèmes d'interprétation des termes contenus dans les délibérations de la CNIL → **risques de mauvaise interprétation pèsent sur le responsable de traitement**

- Pour la durée de conservation : attention à la prise en compte du point de départ et à la définition de « dernier contact » au sens NS 48

- Ouverture d'une newsletter → peut arriver par inadvertance → pas un contact au sens NS 48

MISE EN PLACE DE LISTES D'EXCLUSION ET TRAITEMENT DE DONNEES RELATIVES À DES INFRACTIONS

Analyse de la dernière décision du Conseil d'Etat

LE FONDEMENT LEGAL

- **Art 9 loi I&L : peuvent traiter des données sur les infractions, condamnations, mesures de sûreté:**
  - Les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales
  - Les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi
  - [Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 2004-499 DC du 29 juillet 2004 ;]
  - Les personnes morales mentionnées aux articles L. 321-1 et L. 331-1 du code de la propriété intellectuelle, agissant au titre des droits dont elles assurent la gestion ou pour le compte des victimes d'atteintes aux droits prévus aux livres Ier, II et III du même code aux fins d'assurer la défense de ces droits

LE FONDEMENT LEGAL

- Art 25 I 3° : traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux qui sont mis en oeuvre par des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées

- Art 25 I 4°: Les traitements automatisés susceptibles, du fait de leur **nature**, de leur **portée** ou de leurs **finalités**, d'exclure des personnes du **bénéfice d'un droit**, d'une **prestation** ou d'un **contrat** en l'absence de toute disposition législative ou réglementaire

- La délibération de la CNIL doit être fondée …
- Le REP du responsable de traitement aussi…

LA DELIBERATION DOIT ETRE FONDEE …

- **CE 10ème et 9ème SSR, 23 mai 2007, SACEM et autres, N° 288149**
  - Traitement comportant des infractions
  - *« (…) en estimant que les traitements envisagés conduisaient à une **surveillance exhaustive et continue** des fichiers des réseaux d'échanges et ne pouvaient par conséquent être regardés comme proportionnés à la finalité poursuivie, la CNIL a entaché sa décision d'une erreur d'appréciation »*

LE RECOURS AUSSI….

- **CE 10ème et 9ème SSR, 30 décembre 2009, Experian, N°306173**

  - *« (…) Considérant que la société requérante **ne critique pas utilement** la délibération de la Commission nationale de l'informatique et des libertés au regard du principe de libre concurrence, de celui de libre prestation de service et des objectifs de la directive 95/46/CE du 24 octobre 1995 ;*

  - *Considérant que la circonstance, **qui n'est d'ailleurs étayée par aucun élément et aucune argumentation**, que la Commission nationale de l'informatique et des libertés aurait délivré des autorisations pour des projets de traitements semblables ne constituerait pas, par elle-même, une violation du principe d'égalité (…) »*

L'ANALYSE COMPAREE DES DELIBERATIONS DE LA CNIL

- Pas d'harmonisation dans les visas des délibérations (25 I 3° / 25 I 4°)
- Pas de lignes directrices claires au niveau de la doctrine

L'ANALYSE COMPAREE DES DELIBERATIONS DE LA CNIL

- Le PAYD: ça dépend…
- Prévention des fraudes: autorisée
  - établissement de crédit: délib 2006-244 du 16 nov 2006
- Détection de la fraude documentaire : autorisée
  - Immobilier / établissements de crédit : délib 2008-096 du 10 avril 2008
- Détection de la fraude aux moyens de paiement: autorisée
  - Commerçants: délib 2012-164 du 24 mai 2012 (chèques sans provision)
  - Commerçants VAD: délib 2014-376 du 25 septembre 2014 (CB)
- Prévention de la corruption : autorisée (sous certaines conditions)
  - Délib 2014-486 du 4 décembre 2014

L'ANALYSE COMPAREE DES DELIBERATIONS DE LA CNIL

- Lignes d'alerte éthique: autorisées: attention: seules les lignes d'alerte sont autorisées, pas l'instruction des dénonciations
  - Délib 2013-380 du 5 décembre 2013
- Lutte contre les impayés: autorisée
  - VAD: délib 2012-050 du 16 février 2012
- Pré-contentieux et contentieux civil, commercial, pénal: autorisés
  - Établissement de crédit : délib 2014-106 du 20 mars 2014
- Gestion des audits, du contrôle interne, des risques, des événements et des exigences réglementaires : autorisée (art. 25 I 5°)
  - ADP: délib 2012-396 du 8 novembre 2012
- "Incivilités": autorisées
  - Établissements de crédit : délib 2015-052 du 29 janvier 2015

L'ANALYSE COMPAREE DES DELIBERATIONS DE LA CNIL

- Les autorisations uniques:

- AU 039: fraude à l'assurance
- AU 034: pré-contentieux et contentieux – logement social
- AU 032 : infractions assurances
- AU 026: Ethylotests anti-démarage
- AU 017: pré-contentieux et contentieux – Commerçants – lieux de vente
- AU 014 : prévention des chèques impayés
- AU 011: personnes à risque – location de véhicules
- AU 003: lutte anti-blanchiment

LE CONSEIL D'ETAT

- Principe de sectorisation des listes noires: 28 juillet 2004, 10ème et 9ème SSR, Infobail, N°262851

- CE, 10ème et 9ème SSR, 11 mai 2015, Renault Trucks, N°375669

  - Finalité du traitement : rapprochement consultations de sites à partir des postes informatiques des salariés avec des sites comportant des contenus pédopornographiques communiqués par les autorités de police

  - *« (…) que la société ne conteste pas ne pas être au nombre des personnes mentionnées à l'article 9, qui seules peuvent être habilitées à créer de tels traitements »*

LA PRISE EN COMPTE DES RISQUES DE SANCTIONS EN RECOURANT A DES PRESTATAIRES

Analyse des décisions de la CNIL et du Conseil d'Etat prononçant des sanctions à l'encontre d'entreprises pour des manquements à la loi I&L commis par leurs sous-traitants

RÉGIME JURIDIQUE APPLICABLE

RECOURS À DES SOUS-TRAITANTS :

- **Responsable de traitement** doit assurer la **sécurité et confidentialité des données** traitées (art. 34)

- **Sous-traitant doit présenter des garanties suffisantes** pour assurer la mise en œuvre des mesures de sécurité et de confidentialité de l'art. 34 → **ne décharge pas le responsable du traitement** de son obligation de veiller au respect de ces mesures (art. 35)

- **Contrat entre sous-traitant et responsable du traitement obligatoire**: doit préciser les obligations du sous-traitant en matière de protection de la sécurité et de la confidentialité des données

RÉGIME JURIDIQUE APPLICABLE

- **Responsable de traitement sont sanctionnées pour manquements de leurs prestataires**:

  - Délib. CNIL n° 2013-091 du 11 avril 2013 Total Raffinage Marketing: **avertissement** du responsable de traitement en raison du **non respect** des règles de sécurité et de confidentialité **par son prestataire** de solution de vote électronique

  - Délib. CNIL n°2014-298 du 7 août 2014 ORANGE: **avertissement** du responsable de traitement en raison du **non respect** des règles de sécurité et de confidentialité **par son prestataire** chargé de réaliser ses campagnes marketing

VOTE ÉLECTRONIQUE

Conseil d'Etat, 11 mars 2015, 10ème/9ème SSR n°368748, TOTAL RAFFINAGE MARKETING / E… E…: confirme délibération de la CNIL

- L'utilisation d'un système de vote électronique pour l'élection des délégués du personnel est subordonnée à la **réalisation d'une expertise indépendante** lors :
  - de la conception initiale du système utilisé, et
  - à chaque fois qu'il est procédé à une modification de la conception de ce système, **ainsi que**
  - **préalablement à chaque scrutin recourant au vote électronique**

dernière expertise en 2007 pour des élections en octobre 2012

- la **transmission par simple courriel** des identifiants et mots de passe aux électeurs méconnaissait les obligations de sécurité spécifiques imposées par article R. 2324-5 du code du travail

VOTE ÉLECTRONIQUE

Cass. Soc. 27 février 2013, pourvoi n°12-14415 à propos du système de vote électronique Elections Europe :

*« Qu'en statuant ainsi, alors que **l'envoi de leurs codes personnels d'authentification sur la messagerie professionnelle des salariés**, sans autre précaution destinée notamment à éviter qu'une personne non autorisée puisse se substituer frauduleusement à l'électeur, **n'était pas de nature à garantir la confidentialité des données ainsi transmises**, ce dont il résultait que la conformité des modalités d'organisation du scrutin aux principes généraux du droit électoral n'était pas assurée, le tribunal a violé les textes et principes susvisés »*

- **En ligne avec la position de la CNIL et du CE sur la non-conformité du processus d'envoi d'identifiants et de mots de passe aux dispositions légales applicables**

VOTE ÉLECTRONIQUE

Conseil d'Etat, 11 mars 2015, 10ème/9ème SSR n°372884, Société E…

- injonction à la présidente de la CNIL de procéder à l'anonymisation des mentions de la délibération n° 2013-091 du 11 avril 2013 de la formation restreinte de la CNIL concernant la société E... dans un délai de quinze jours à compter de la notification de la présente décision

- la CNIL versera à la société E... une somme de 3 000 euros au titre des dispositions de l'article L. 761-1 du CJA.

VOTE ÉLECTRONIQUE

CE QU'IL FAUT EN RETENIR:

- Une expertise indépendante et **préalable à chaque scrutin est nécessaire**

- **L'envoi des identifiants et mots de passe par mail n'est pas conforme** aux mesures exigées par la loi

- **Circonstances inopérantes:**

  - le juge judiciaire aurait reconnu la fiabilité du système de vote
  - l'accord avec les organisations syndicales a été signé
  - aucune atteinte aux données ni aux principes du droit électoral relevé pour les élections concernées
  - absence de contestation du résultat des élections

FAILLES DE SÉCURITÉ

Délibération CNIL n°2014-298 du 7 août 2014 ORANGE (1/2)

- Faille de sécurité notifiée à la CNIL : dysfonctionnement du serveur d'un prestataire → un tiers non autorisé accède aux données : 1 340 000 clients impactés

- Responsable de traitement a l'obligation d'assurer la confidentialité et la sécurité des données de ses clients et prospects et **ne peut pas limiter sa responsabilité par le recours à des prestataires**

- Responsable de traitement n'a pas fait réaliser d'audit de sécurité sur une application technique spécialement développée par le prestataire pour ses besoins

FAILLES DE SÉCURITÉ

Délibération CNIL n°2014-298 du 7 août 2014 ORANGE (2/2)

- Responsable de traitement communiquait de manière non sécurisée les mises à jour ses fichiers clients et prospects à ses prestataires
- Aucune clause de sécurité et de confidentialité des données n'était imposée à son prestataire "secondaire"
- **Mesures mises en oeuvre en termes de sécurité des données avant la faille étaient insuffisantes** et ont contribué à la récupération des données par un tiers malveillant

RECOURS A DES SOUS-TRAITANTS

- **Problématiques rencontrées par les responsables de traitement:**

  - Ne **disposent pas de l'expertise technique** leur permettant parfois de s'assurer de la mise en place de mesures de sécurité et de confidentialité adéquates

  - Le **prestataire refuse de modifier les modalités** de mise en œuvre du traitement et notamment les mesures de sécurité et de confidentialité

    → arguments avancés:

      - solution clé en main, coûts, etc
      - réserves du responsable de traitement injustifiées

RECOURS A DES SOUS-TRAITANTS

CE QU'IL FAUT EN RETENIR:

- Le **risque et les sanctions** en cas de défaut de sécurité et de confidentialité **pèsent sur le responsable de traitement**, peu importe la qualification dans le contrat

- **Vérifications / Conseils:**
  - Faire appel à des personnes compétentes pour vérifier les mesures de sécurité (RSSI, expert,etc)
  - Insérer des clauses adéquates dans le contrat relatives aux obligations de sécurité et confidentialité des données
  - Insérer une clause d'audit et réaliser des audits réguliers auprès des prestataires

MERCI

helene.lebon@pdgb.com
sandra.tubert@pdgb.com
PDGB Société d'Avocats
174 avenue Victor Hugo
75116 Paris
Tel: 01 44 05 37 34
Fax: 01 44 05 21 00
www.pdgb.com