

Zoom

CARLARA
& international
SELECTED FULL SERVICE LAW FIRMS

LA NEWSLETTER DE CARLARA INTERNATIONAL

ÉDITORIAL

RGPD, DPO : CIA ? KGB ? DGSE ?

« *In wartime, truth is so precious that she should always be attended by a bodyguard of lies.* » (Winston Churchill)

On dit souvent que l'argent est le nerf de la guerre.

On pourrait dire la même chose de l'information : c'est celui qui possède le plus d'informations sur l'autre qui gagnera le combat.

Cette information peut être protégée de deux manières : en la cachant, ou bien en la multipliant de telle sorte qu'elle soit inexploitable.

Chaque avocat se souvient d'avoir reçu d'un adversaire, dans une procédure complexe, des caisses entières de pièces sans pertinence dans lesquelles étaient noyés deux ou trois documents gênants.

Le monde actuel se manifeste par l'explosion des données et notamment des données personnelles : votre état civil, vos goûts, vos dégoûts, vos vacances, vos loisirs préférés, dont l'exploitation explose du fait des outils informatiques existants.

Les données innombrables (la Big Data), combinées à la puissance quasi infinie d'Amazon ou de Google, deviennent une véritable arme de destruction massive ; une arme commerciale car elle permet de cibler chacun jusque dans ses plus petits secrets, et une arme politique contre les libertés : on a vu récemment dans la presse les photos de policiers chinois munis de lunettes à réalité augmentée qui permettent de reconnaître dans une foule les individus qui sont fichés ou recherchés grâce à des mécanismes de reconnaissance faciale !

Face à ces évolutions vertigineuses et notamment face à « l'impérialisme » de l'économie américaine qui impose ses règles juridiques au monde entier tout en piochant dans le vaste champ de données de centaines de millions de consommateurs, l'Union Européenne a mis en œuvre, par un règlement dit Règlement Général de Protection des Données (RGPD), un certain nombre de garde-fous et de barrières.

L'idée en un mot est de permettre aux particuliers de garder, au moins partiellement, la maîtrise de leurs données, et de contraindre les entreprises à mettre en place des procédures permettant cette maîtrise.

C'est l'objet du RGPD.

Dans chaque entreprise, devra être nommé un Délégué à la Protection des Données (DPD), souvent appelé DPO (Data Protection Officer). Toute entreprise qui traite de manière régulière, systématique et à grande échelle des données à caractère personnel de clients, salariés, etc. doit nommer un DPO (parmi les sociétés les plus visées, figurent bien évidemment les banques, secteur qui connaît particulièrement bien ses clients [habitudes d'achats, localisation des retraits, situation familiale, nombre d'enfants, etc.]).

L'Union Européenne s'est donnée les moyens de faire appliquer le RGPD puisque, par exemple, une banque qui n'aurait pas désigné son DPO encourt une amende administrative pouvant atteindre 20 millions d'euros ou 4% du chiffre d'affaires mondial de l'exercice précédent.

Le rôle du DPO va bien au-delà de la mission confiée à l'ancien correspondant informatique et liberté dont la nomination était par ailleurs facultative. Le DPO conseille et informe la société quant à ses obligations, il supervise la conformité de l'entreprise avec le RGPD et veille à la tenue du registre de traitement et la gestion des audits de conformité.

Il conseille également l'entreprise quant à la nécessité de mener une étude d'impact sur la protection des données et sera l'interlocuteur des clients lorsqu'ils déposent une réclamation relative à l'utilisation de leurs données personnelles.

Il est préférable de ne pas choisir le DPO à l'intérieur du personnel de l'entreprise, et cela pour des raisons évidentes : d'un niveau trop élevé, il pourra être suspecté de conflit d'intérêt ; d'un niveau trop faible, il n'aura pas l'autorité et les pouvoirs nécessaires pour agir.

C'est la raison pour laquelle certains cabinets d'avocats se sont lancés dans cette activité qui requiert indépendance, capacité à écouter et à convaincre les instances décisionnaires ainsi qu'une véritable expertise juridique.

Le caractère de profession réglementée de la profession d'avocat permet évidemment aux entreprises qui font appel à lui de bénéficier de toutes les assurances correspondantes, au sens propre comme au sens figuré.

En conclusion, la mise en conformité aux exigences du RGPD et la nomination d'un DPO ne sont pas une option pour les entreprises et notamment les banques, dont le secteur ultra concurrentiel est régulièrement « challengé » par l'arrivée de nouveaux acteurs (banques en ligne, opérateurs téléphoniques) et dans lequel la qualité de la relation client est désormais un atout majeur.

Par ailleurs, au-delà de la contrainte qu'elle représente, la nomination d'un DPO est aussi une opportunité pour démontrer à ses clients qu'une entreprise est à la hauteur de son rôle éventuel de tiers de confiance, en mettant en place une véritable politique de gestion et de contrôle des données personnelles, en communiquant sur l'utilisation faite de ces données et en permettant à leurs clients d'exercer leurs droits issus du RGPD.



Michel RASLE
Avocat associé CARLARA

AU SOMMAIRE

QUELLES SANCTIONS EN CAS DE NON-CONFORMITÉ ?	PAGE 2
COMMENT RÉAGIR EN CAS DE CONTRÔLE ?	PAGE 3
ACTUALITÉS - CONFÉRENCES - ARTICLES - COLLOQUES	PAGE 4

QUELLES SANCTIONS EN CAS DE NON-CONFORMITÉ ?

Le montant des amendes que la Commission Nationale de l'Informatique et des Libertés (CNIL) peut infliger aux entreprises ne respectant pas la législation relative à la protection des données à caractère personnel a été significativement augmenté par le RGPD. En effet, la dite « loi Informatique et Libertés » du 6 janvier 1978 telle que modifiée par la loi du 6 août 2004 prévoyait que la CNIL ne pouvait prononcer des sanctions supérieures à 150 000 euros pour un premier manquement.

Quels sont la nature et le montant des sanctions ?

La loi pour une République numérique du 7 octobre 2016 est venue hisser le plafond de 150 000 euros à 3 millions d'euros afin d'anticiper la mise en place par le RGPD d'un plafond bien supérieur. En effet, la responsabilisation des entreprises par le RGPD s'accompagne de sanctions beaucoup plus importantes. Ainsi, en cas de manquement au « privacy by design » ou encore en matière d'analyse d'impact, l'entreprise encourt une amende pouvant aller jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial. Le manquement aux droits des personnes (droit à l'information, droit d'accès, droit à l'oubli, etc.) est réprimé plus sévèrement, l'entreprise encourant alors une amende pouvant aller jusqu'à 20 millions d'euros ou 4% de son chiffre d'affaires annuel mondial.

Les sanctions prononcées par la CNIL peuvent s'accompagner de sanctions pénales. Il existe dix-neuf incriminations prévues par les articles 226-16 et 226-24 du Code pénal qui punissent notamment de 5 ans d'emprisonnement et de 300 000 euros d'amende le fait de procéder à des traitements de données à caractère personnel sans respecter les formalités préalables à leur mise en œuvre et le fait de conserver des données sensibles (données de santé, opinions politiques, origines raciales ou ethniques, etc.) sans le consentement de la personne concernée. L'article 131-39 du Code pénal ajoute à l'encontre des personnes morales des sanctions spécifiques telles que : interdiction temporaire ou définitive d'exercice, exclusion des marchés publics, etc.

Cette responsabilité pénale s'accompagne d'une responsabilité civile dans la mesure où l'article 82 du RGPD prévoit que toute personne ayant subi un dommage matériel ou moral en raison de la violation du Règlement a le droit à la réparation du préjudice subi. La responsabilité du responsable de traitement peut aussi être engagée sur le fondement du droit commun de la responsabilité civile (article 1240 du Code civil).

Quelles sanctions ont été prononcées à ce jour ?

La CNIL a prononcé le 8 janvier 2018 une sanction d'un montant de 100 000 euros à l'encontre de la société DARTY au motif qu'elle avait manqué à son obligation de sécurité des données à caractère personnel de ses clients. La Commission précise, en outre, que le simple fait d'avoir

recours à un prestataire sous-traitant ne décharge pas la société de ses obligations.

Le 7 mai 2018, la CNIL a prononcé une sanction de 250 000 euros à l'encontre de la société OPTICAL CENTER qui avait manqué à son obligation de sécurité des données. Dans cette affaire, il y avait eu une fuite de données. La CNIL souligne dans sa décision que la société ne pouvait ignorer le défaut de sécurisation dans la mesure où elle avait déjà été condamnée en 2015 à 50 000 euros d'amende en raison d'un défaut de sécurité.

Le 21 juin 2018, une sanction de 75 000 euros a été prononcée à l'encontre de l'Association pour le Développement des Foyers pour avoir insuffisamment protégé les données des utilisateurs de son site internet.

Les premières sanctions prononcées en 2018 montrent un accroissement significatif du montant des sanctions prononcées, même si, pour l'instant, ces sanctions sont prises en vertu de la loi ancienne, car elles concernent des faits antérieurs à l'entrée en application du RGPD.

Ces trois décisions ont été prises sur le fondement de l'article 34 de la loi Informatique et Libertés qui impose une obligation de sécurité des données personnelles. Cette obligation est une obligation fondamentale que l'on retrouve dans le RGPD et dans la loi Informatique et Libertés modifiée. Ces décisions auraient sans aucun doute été similaires si elles avaient été prises sur le fondement du RGPD. La seule différence aurait pu se situer au niveau du montant des amendes infligées.

Par ailleurs, en vertu du RGPD, les personnes concernées peuvent se faire représenter par des associations ou des organismes actifs dans le domaine de la protection des données personnelles pour exercer en leur nom une réclamation auprès de la CNIL. C'est ainsi que l'association la Quadrature du Net a déposé, le 28 mai 2018, une réclamation collective auprès de la CNIL concernant les GAFAM (Google, Apple, Facebook, Amazon et Microsoft) au nom de plus de 12 000 personnes. Ces réclamations sont toutes fondées sur la licéité du traitement des données, pierre angulaire du RGPD. En effet, l'association estime notamment que le consentement des internautes n'est pas libre et éclairé. Or, la question du consentement concerne toutes les entreprises quelle que soit leur taille. Ces réclamations déposées seulement trois jours après l'entrée en vigueur du RGPD invitent les entreprises à se mettre en conformité. Ces réclamations qui ne sont que la partie cachée de l'iceberg montrent, comme l'affirme Isabelle Falque-Pierrotin, la présidente de la CNIL, que « *le grand public est intéressé par toutes les obligations de transparence, le consentement et tous les nouveaux droits.* » L'entreprise doit désormais en tenir compte.



Clarisse LE SALVER
Avocat CARLARA

COMMENT RÉAGIR EN CAS DE CONTRÔLE ?

Le nombre de plaintes auprès de la CNIL ne cesse d'augmenter depuis l'entrée en vigueur du RGPD. Cette augmentation des plaintes pourra s'accompagner d'une augmentation des contrôles même si la CNIL prévoit d'effectuer le même nombre de contrôles en 2018 qu'en 2017.

Qui est concerné par les contrôles ?

Toute entreprise qui effectue des traitements de données personnelles, quelle que soit sa taille, peut faire l'objet d'un contrôle de la CNIL dès lors qu'elle dispose d'un établissement situé sur le territoire français ou recourt à des moyens de traitement situés en France. La décision de contrôler une entreprise peut avoir plusieurs origines dont notamment les réclamations et signalements adressés à la CNIL par tout intéressé.

En outre, dans le cas d'un traitement transfrontalier de données à caractère personnel au sein de l'Union européenne, le RGPD prévoit un mécanisme d'autorité de contrôle dite « chef de file ». Cette autorité est en principe seule compétente pour ce type de traitement : elle se substitue donc aux autres autorités de contrôle concernées, tout en coopérant avec elles. L'autorité chef de file compétente sera celle située dans l'État où l'entreprise a son centre de décision. Par exemple, pour Facebook, l'autorité compétente sera l'autorité irlandaise dans la mesure où Facebook a son siège social en Irlande. Cette innovation du RGPD souligne la force politique qui est donnée à la protection des données à caractère personnel. De plus, l'article 62 du RGPD permet à plusieurs autorités de contrôle de réaliser des enquêtes conjointes. Le caractère européen de la législation prend ainsi tout son sens.

Quels contrôles ?

L'article 58 du RGPD et l'article de la loi Informatique et Libertés prévoient quatre types de contrôles : sur place, sur pièces, sur convocation et en ligne. La CNIL est libre d'utiliser un ou plusieurs de ces contrôles à sa convenance. En tout état de cause, ces contrôles visent à obtenir le maximum d'informations techniques et juridiques qui permettront à la CNIL d'apprécier les conditions de mise œuvre du traitement. La CNIL pourra ainsi avoir accès à toutes les données à caractère personnel, à toutes les informations nécessaires à l'accomplissement de ses missions et à tous les locaux du responsable de traitement et de ses éventuels sous-traitants.

Quelle différence entre les contrôles ?

Le contrôle sur place permet aux agents de la CNIL d'avoir accès, de 6 heures à 21 heures, aux lieux, locaux, enceintes, installations ou établissement de l'entreprise qui servent à mettre en œuvre le traitement. Le procureur de la République doit être préalablement informé du contrôle. En outre, le responsable des lieux est informé de son **droit d'opposition à la visite**. S'il exerce ce droit, la visite devra être autorisée par le Juge des Libertés et de la Détention (JLD) (article 44

de la loi Informatique et Libertés). Cependant, en cas notamment d'urgence ou de risque de destruction ou de dissimulation de documents, le JLD pourra être saisi aux fins d'autoriser de manière préalable la visite. Dans une telle hypothèse, le responsable des lieux ne pourra pas s'opposer à la visite n'étant pas informée de celle-ci, mais pourra saisir à tout moment le JLD ayant autorisé la visite d'une demande de suspension ou d'arrêt de la visite.

Le contrôle sur pièces permet à la CNIL de demander la communication de tous documents quel qu'en soit le support et d'en prendre copie.

Le contrôle sur convocation permet à la CNIL de recueillir auprès de toute personne tout renseignement et toute justification utiles et nécessaires.

Le contrôle en ligne s'effectue par la CNIL via une plateforme et une connexion internet dédiées. L'information préalable du responsable de traitement n'est pas systématique. Il se limite à la consultation des données librement accessibles ou rendues librement accessibles par imprudence, négligence ou le fait d'un tiers. Ce contrôle permettra à la CNIL de vérifier si l'entreprise respecte la législation relative à la collecte des données à caractère personnel : mesures de sécurité suffisantes, présence des mesures d'information, voire de consentement, respect des dispositions réglementaires en matière de cookies, etc.

Que faire en cas de contrôle ?

Lorsque l'entreprise fait l'objet d'un contrôle de la CNIL, il est primordial que l'entreprise informe immédiatement son délégué la protection des données (en anglais : « *Data Protection Officer* » - DPO) et son avocat.

L'entreprise se doit, ensuite, de coopérer avec les services de la CNIL et de répondre à leurs questions. Cependant, l'entreprise doit préférer réserver sa réponse et consulter son conseil si elle estime ne pas être en mesure de répondre de façon satisfaisante aux questions posées.

L'entreprise doit, en outre, être réactive et prendre des mesures rapides pour remédier au manquement constaté. Ainsi, une entreprise ayant fait preuve de coopération est susceptible de voir le montant de la sanction initialement prévue diminuer de manière considérable. L'article 83 du RGPD impose en effet à la CNIL de notamment prendre en compte « *le degré de coopération avec la CNIL en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs* » et « *toute mesure prise pour atténuer le dommage subi par les personnes concernées.* » Par exemple, dans l'affaire concernant DARTY, la CNIL a tenu compte de l'initiative du responsable de traitement de diligenter un audit de sécurité après l'atteinte à la sécurité des données et sa bonne coopération avec les services de la CNIL.

ACTUALITÉS

L'équipe corporate du Cabinet figure dans le classement 2018 d'Option Droit & Affaires des cabinets d'avocats en M&A.

Alban CURRAL, spécialiste en droit économique, rejoint le Cabinet en qualité d'associé au sein du Pôle Concurrence, Distribution. Après avoir exercé à Bruxelles et à Philadelphie (Pennsylvanie, États-Unis), Alban CURRAL a développé ses activités au sein de cabinets d'affaires parisiens auprès d'une clientèle française et étrangère, incluant des sociétés privées et publiques dans divers secteurs dont la grande distribution, l'industrie, la cosmétique. Il intervient également dans les dossiers réglementation produits et assiste des entreprises nationales et internationales pour les questions concernant REACH, CLP, WEE et RoHS. Cette activité inclut des missions de lobbying auprès des Autorités locales, nationales et européennes.



Après plusieurs stages au sein de cabinets d'avocats, de collectivité territoriale et de juridiction administrative, **Guillaume VAN HOUTTE** a rejoint le département Droit public du Cabinet, en qualité de collaborateur, à l'issue de son stage final. Inscrit au Barreau de Paris, il est diplômé de l'Université de Lille II (Master II Droit public de l'économie) et de l'Université Paris II – Panthéon Assas (Master II Vie publique et relations institutionnelles).



Valentin LE DILY a rejoint le département droit social du Cabinet en juillet, en qualité d'avocat collaborateur. Il est diplômé de l'Université Paris Dauphine (Master II Droit Européen et International des affaires, 2012) et de la Saint Louis University (LLM, 2013). Après avoir été directeur général d'une association nationale, il a exercé au barreau de New York comme avocat avant de prêter serment au barreau de Paris en juillet 2018.



Inscrite au Barreau de Paris en 2018, **Claire DAOU DAL** a rejoint le département pénal du Cabinet en qualité de collaboratrice. Elle est diplômée du Master de droit pénal et pratique du droit pénal de l'Université Paris XI. Avant de rejoindre le Cabinet, elle a effectué de nombreux stages dans des cabinets d'avocats, en juridiction et à l'étranger.



CARLARA INTERNATIONAL - www.carlara.com
CARBONNIER LAMAZE RASLE & ASSOCIÉS
8, rue Bayard - 75008 Paris

CARLARA LILLE
21, boulevard du Général Leclerc - 59100 Roubaix

CARBONNIER LAMAZE RASLE & ASSOCIÉS BRUXELLES
Avenue Louise 235 - B - 1050 Bruxelles

CARLARA BRUXELLES
Boulevard Saint-Michel 11 - B - 1040 Bruxelles

CARLARA SOCIAL (anciennement ALCIMUS AVOCATS)
8, rue Bayard - 75008 Paris
55, rue du Président Edouard Herriot - 69002 Lyon

PREUILH VIDONNE CROIZAT HUGUENIN & ASSOCIÉS
55, rue du Président Edouard Herriot - 69002 Lyon



Inscrite au Barreau de Paris en 2017, **Marion DIEBOLD** a exercé pendant un an avant de rejoindre le Cabinet en qualité de collaboratrice et intervient en contentieux bancaire. Elle est diplômée d'un Master I en Droit des affaires et d'un Master II en Droit des contentieux et de l'exécution.

CONFÉRENCES - ARTICLES - COLLOQUES

Hedwige CALDAIROU a collaboré à la rédaction de la deuxième édition paru en décembre 2018, de l'ouvrage de référence en matière de médiation, « *Art et Technique de la médiation* », publié par les éditions LexisNexis sous la direction de Stephen Bensimon (philosophe et médiateur), Martine Bourry d'Antin (avocat et médiateur) et Gérard Pluyette (magistrat, prescripteur).

Elle a co-écrit avec Catherine Peulvé, Membre élue du CNB (2018-2020), Vice-présidente nationale de l'ACE et Présidente d'honneur de l'ACE Paris le chapitre consacré à la médiation interentreprises.

Le 19 octobre 2018, à Lyon, **Antoine FOURMENT** est intervenu comme animateur d'un atelier consacré au futur du financement des cabinets d'avocats et aux principes d'élaboration des business plans dans le cadre des États généraux de la prospective et de l'innovation du Conseil National des Barreaux.

Frédéric HUGUENIN, Avocat Associé CARLARA LYON, a participé le 8 novembre dernier à une table ronde organisée par Lyon Place Financière et Tertiaire ayant pour thème : « *Financements désintermédiés : Invitation à la découverte d'une offre qui s'élargit et se simplifie* ».

Edouard de LAMAZE s'est vu confier début juillet par Madame la Garde des Sceaux, une mission sur l'avenir de la profession d'opérateurs de ventes volontaires, aux côtés de Madame Henriette Chaubon. Après avoir mené ces derniers mois une série d'auditions à la Chancellerie, leur rapport a été remis à Madame la Ministre le 20 décembre 2018.

Hervé LECUYER a participé le 24 août à un colloque organisé par l'IJLS à Port-Louis (Ile Maurice) sur le thème de la copropriété, le 26 septembre, il a dispensé une formation continue à l'Ecole Nationale de la Magistrature, portant sur le droit de l'assurance-vie et le droit des successions. Le 11 octobre, il est intervenu à un Colloque COVEA sur le thème des véhicules autonomes.

Guillaume de RUBERCY a publié en juin 2018 l'éditorial pour l'Observatoire économique francophone du Forum Francophone des Affaires (FFA) intitulé : « *Bref comparatif des trois principaux règlements d'arbitrage : CIRDI, CNUDCI et CCI - Outil(s) de protection en matière d'investissement* ».

ZOOM
LA NEWSLETTER DE CARLARA INTERNATIONAL - N° 32

DIRECTEUR DE LA RÉDACTION : ÉDOUARD DE LAMAZE.
ONT PARTICIPÉ À CE NUMÉRO : MICHEL RASLE,
CLARISSE LE SALVER, CLAIRE CHAILLOU,
ANTOINE FOURMENT.

MAQUETTE : APALOZA. IMPRESSION : ATELIERS 30.