Un règlement européen pour mieux sécuriser nos données personnelles

Dossier réalisé par Patrick Vancampenhout

- Le Règlement général sur la protection des données (RGPD) entre en vigueur ce vendredi.
- Il s'agit d'une adaptation plus "numérique" des anciennes règles.
- C'est un défi pour les entreprises qui doivent se conformer.

C'est l'agitation dans les entreprises, ces jours-ci. Un nouveau cadre légal européen relatif à la protection des données privées entre en effet en vigueur ce vendredi. Le RGPD, pour "Règlement général sur la protection des données", est une nouveauté majeure. Ce règlement qui doit être appliqué dans les pays de l'Espace économique européen (les pays de l'Union plus l'Islande, la Norvège et le Liechtenstein), est une sérieuse mise à jour des dispositions existantes (directive européenne 95/46). D'autant qu'elles sont intégrées simultanément dans le droit des pays membres. En conséquence, de nombreuses entreprises envoient des courriels demandant à leurs contacts de consentir à l'utilisation de leurs données. Si vous être indépendant, patron d'une PME ou dirigeant d'une ASBL et que vous découvrez cette information, sachez qu'il n'y a pas matière à paniquer. Vous n'aurez pas demain la visite d'un inspecteur en charge de constater d'éventuels manquements par rapport au RGPD...

L'instauration de ce nouveau cadre va surtout vous demander une réflexion sérieuse sur le type de données récoltées, la manière dont elles le sont, leur traitement et leur sécurisation dans l'intérêt de vos contacts. *"Bien entendu, le cas d'une PME informatique qui gère ses contacts clients et celui d'une entreprise de marketing qui récolte et croise des données 'sensibles'à des fins commerciales, sont fondamentalement différents"*, nous explique François Bryssinck, CEO de la société informatique Megabyte. *"Un peu de réflexion et un peu de travail administratif devraient suffire dans la plupart des cas. Il est probable que les entreprises disposant de données sensibles ont depuis longtemps songé aux risques, et à la manière de sécuriser leurs données."*

1 Le RGPD, c'est quoi exactement ?

Le RGPD, qui entre en vigueur ce 25 mai, est en fait le "Règlement général sur la protection des données". Il s'agit d'un texte de loi s'appliquant uniformément dans les pays de l'Espace économique européen (EEE), soit les 28 pays membres de l'Union européenne plus la Norvège, l'Islande et le Liechtenstein. Il offre une standardisation des règles de protection des données des particuliers, qui simplifie le travail des entreprises exposées auparavant à des réglementations locales issues de la transposition de la directive 95/46. Mais il impose aussi une série de règles assez strictes sur la récolte des données, leur traitement, leur utilisation, leur sécurisation, le tout avec l'approbation claire des personnes. On parle ici surtout de fichiers clients dans le cadre de leurs relations avec les entreprises, publiques ou privées. L'objet de ce texte est d'adapter la loi à l'existence des entreprises Internet. Le RGPD instaure aussi une autorité locale ayant un pouvoir de sanction important. En Belgique, l'Autorité de protection des données remplace ainsi la Commission de la vie privée.

2 Quelles sont les données personnelles visées par le RGPD ?

Toutes les données récoltées sur des personnes, permettant de les identifier, sont des données sensibles visées par le RGPD. En ce compris, des caractéristiques révélant l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance à des groupes comme des syndicats. On parle aussi de données relatives à l'orientation sexuelle, aux données biométriques ou génétiques. Pratiquement, le traitement ou l'exploitation de ces données, sont interdits... sauf si la personne avertie clairement sur l'utilisation de ses données a donné son consentement à leur traitement. Les personnes doivent pouvoir accéder à leurs données, les modifier ou les supprimer, sauf si le droit national s'y oppose (conservation de factures dans la comptabilité, par exemple). Notons que pas mal de données privées sont aisément disponibles en ligne, comme la foule de celles présentes sur les réseaux sociaux. Ce qui en dit long sur le peu de conscience qu'ont les particuliers de leur importance.

3 Quels sont les principaux droits des internautes ?

Les internautes qui remplissent des formulaires en ligne doivent être informés de manière claire de ce que l'entreprise fait avec leurs données. L'entreprise doit limiter ses demandes de données à celles qui sont expressément utiles à l'utilisation qu'elle compte en faire. Les entreprises doivent mettre en place des procédures permettant aux particuliers de recevoir une copie de leurs données, de les modifier, de les supprimer (droit à l'oubli) et de les transférer (pour passer d'un réseau social à un autre, par exemple). Dans la plupart des cas, bien entendu, les clients accepteront volontiers le traitement de leurs données par les entreprises avec lesquelles ils entretiennent de bons rapports.

4 Le profilage commercial sera-t-il moins intense ?

S'il semble à première vue que les particuliers seront moins bien ciblés par les campagnes publicitaires, ce ne sera probablement pas le cas en pratique. Les spécialistes du traitement des données ont évidemment anticipé le RGPD et ce nouveau cadre est considéré par certains comme une manière de nettoyer leurs bases de données et de repenser leur traitement sur des bases plus saines et plus éthiques. Fondamentalement, on sait que les consommateurs apprécient la publicité ciblée, si elle correspond précisément à leur profil. Pourtant, le Syndicat neutre pour indépendants (SNI) a réalisé une étude à propos des envois d'e-mails publicitaires et estime que *"42 pour cent des entreprises n'enverront plus ces e-mails et 21 pour cent en diminueront la fréquence d'envoi"*. Jusqu'au moment où elles auront mieux cerné les contours du RGPD ?

5 Toutes les entreprises sont-elles concernées ?

Dès lors qu'une entreprise, même si son siège est situé hors de l'Espace économique européen, recueille des données à propos de ses clients, elle doit les traiter dans le cadre défini par le RGPD. Elle doit aussi s'assurer que ses sous-traitants auxquels elle livre une partie des informations sur ses clients respectent le Règlement européen. Une fois encore, si le cadre a changé, il ne s'agit pas ici d'une révolution pour les entreprises qui gèrent les données de manière raisonnable. Quelques ajustements seront nécessaires, mais il n'y a pas lieu de paniquer. Les entreprises envoient pourtant actuellement des courriels à leurs clients ou contacts, demandant d'accepter les conditions de traitement de leurs données. Pour François Bryssinck (Megabyte), *"il n'y a ici qu'une obligation de moyens..."*

6 Quid des autres opérateurs (ASBL, administrations...) ?

Les responsables d'ASBL sont concernés par le Règlement dans la mesure où ils gèrent des bases de données relatives à leurs membres. Même les Eglises doivent l'appliquer. Les administrations sont également tenues aux obligations d'accès et de transparence, dans la mesure où ces obligations ne contreviennent pas à leurs missions de base.

Difficile d'imaginer que la Sûreté de l'Etat vous donne accès à ce qu'elle sait à votre propos et vous permette de modifier les données ou de les faire disparaître... Dans le cas contraire, le Règlement est d'application. Un exemple ? Les abonnés à la lettre d'information de la Cour constitutionnelle ont reçu jeudi un e-mail leur proposant de se réinscrire, en demandant simplement de retaper leur adresse électronique et en spécifiant que celle-ci ne serait pas utilisée à d'autres fins que l'envoi des lettres reprenant les derniers arrêts prononcés par la Cour.

7 Les Gafa sont-ils particulièrement sous pression ?

L'affaire Cambridge Analytica ou le piratage des données de Yahoo ont mis en lumière l'importance des données manipulées par les grands groupes de l'économie Internet (les Gafa, pour Google, Apple, Facebook et Amazon). Ces groupes sont évidemment les cibles visées par cette nouvelle législation. Lors de l'audition cette semaine du patron de Facebook, Mark Zuckerberg, certains ont rappelé le risque d'un usage illégal des données des membres, utilisateurs ou clients. Les sanctions peuvent se monter jusqu'à 20 millions d'euros ou à 4 % du chiffre d'affaires mondial des contrevenants... Inutile de dire que les juristes et les informaticiens des Gafa ont dû passer des nuits blanches pour adapter leurs systèmes de gestion des données privées. Zuckerberg a assuré que Facebook serait en ordre... ce vendredi. Surtout, cette législation européenne force pratiquement ces géants à utiliser le RGPD comme base de leur politique de gestion partout dans le monde.

8 Les entreprises belges sont-elles préparées ?

Comme le révélait "La Libre" la semaine passée, une enquête menée par l'Agence wallonne du numérique (AdN) a montré que près d'une entreprise wallonne sur deux n'était pas au courant de l'entrée en vigueur de la nouvelle législation européenne sur le traitement des données. Mais il faut dire que la sensibilité de ces dernières est fonction de leur secteur d'activité et de leur taille. Les grandes entreprises belges ont déjà avancé sur ce chantier. Les multinationales américaines actives en Europe avaient intégré le RGPD dans leur planning 2017. Mais la Belgique est avant tout une terre de PME, d'associations sans but lucratif (ASBL), focalisées sur leurs objectifs plus que sur une législation opaque pour le commun des mortels. La masse d'informations dispensée ces jours-ci devrait toutefois susciter chez de nombreux responsables d'entreprises une réflexion suivie d'action.

9 Quel est le rôle du "DPO" au sein des entreprises ?

Le "Data Protection Officer", "DPO" ou "délégué à la protection des données", est une personne importante dans la gestion de la transformation des entreprises qui doivent intégrer la nouvelle dimension du traitement des données privées. Dans une PME, ce sera souvent le patron ou l'informaticien, même à temps partiel. Dans les structures sans candidat évident, on fera appel à des consultants (le RGPD est pour ces derniers du pain bénit). Dans les entreprises plus importantes, on tentera de trouver un juriste initié à l'informatique ou l'inverse. En tout cas, un profil ouvert, très au fait du fonctionnement de l'entreprise et capable d'endosser la responsabilité à temps plein. Il existe des formations courtes, d'une ou deux semaines, pour former des candidats. Et selon des chiffres récents, près de 30 000 postes de DPO devraient être créés en Europe.

10 Qui va contrôler la bonne application du RGPD ?

La Commission vie privée disparaît au profit de l'Autorité de protection des données (APD). C'est auprès de cet organe qu'il faudra se tourner en cas de problème, avec les données des particuliers, en cas de piratage d'une base de données, pour signaler les faits. Cette autorité dispose de moyens accrus comme la possibilité d'imposer des sanctions (avec bien entendu une possibilité d'appel), ce qui lui permet de gérer les cas plus rapidement qu'auparavant, lorsqu'elle devait passer par les tribunaux. Il s'agit donc là d'un véritable tribunal (au sein de l'organe nommé "Chambre contentieuse"), mais, avant tout, l'APD est une source d'information de première main (Centre de connaissances), où l'on pourra trouver de l'aide et des conseils (en ligne, notamment). Inutile d'imaginer le déploiement d'une armée de limiers chargés de traquer le format des demandes d'abonnement à la feuille d'information des scouts du coin. L'APD elle-même pourra se référer à un organe supranational, le Comité européen de la protection des données, pour valider des décisions nationales avant leur adoption.