N°109 I juin 2018 I Fr.6.-

le magazine de la fédération romande des consommateurs

INDÉPENDANT ET SANS PUBLICITÉ DEPUIS +50 ans

frc mieux choisir

Vie privée
Qui joue avec nos données ?

santé

App cosmétiques
La FRC se lance dans le crowdfunding

test

Végétarisme
Les galettes méritent peu d'éloges

édito

Le feu est à l'orange

Laurence Julliard

La nouvelle est fraîche, elle est tombée le 27 mai. Les coopératives Migros ont pris l'engagement par voie de presse de se conformer aux exigences du Règlement général européen sur la protection des données (RGPD). Voilà qui tombe à point nommé pour les détenteurs de la carte Cumulus en Suisse comme pour ceux qui se rendent dans l'une de ses enseignes à l'étranger.

Mais concrètement, que signifie cette déclaration d'intention? Spontanément, on a envie de croire que la nouvelle est réjouissante, que les clients bénéficieront désormais d'un bon garde-fou quant à l'utilisation des informations qu'ils auront bien voulu transmettre au géant orange pour bénéficier d'avantages. De l'avis des professionnels du droit, en effet, ce RGPD est un cadre qui sert au mieux les intérêts des consommateurs. Un vrai bouclier. Une première mondiale, qui explique pourquoi tout le monde ne parle que de ça.

Il se trouve que notre dossier du mois est justement consacré à cette épineuse question: comment notre quotidien est-il affecté par les données que nous laissons échapper de gré ou de force tout au long de la journée? Hasard du calendrier, Cumulus et Supercard figurent en bonne place, évidemment. Un collaborateur de la FRC, au bénéfice de ces cartes fidélité, a justement demandé à avoir accès à ses données pour se rendre compte du profilage qui était fait de son ménage. Ce travail de l'ombre, certes réalisé en début d'année quand les entreprises helvétiques toussaient encore à l'idée de se mettre en conformité avec le droit européen, montre tout de même deux choses: le client livre de précieux renseignements mais lorsqu'il demande la pareille en retour, il se heurte à un mur. Autre constat, comme les actions ou rabais intéressants sont de plus en plus liés à une carte, les petits revenus n'ont d'autre choix que de passer par là. Sous cet angle, le consentement volontaire et explicite du consommateur prend une drôle de signification.

Inutile de brandir trop rapidement le carton rouge. Il va falloir prendre la mesure du temps, attendre les leçons tirées de quelques jurisprudences pour évaluer la part des gains dont nous aurons profité et des pertes que nous aurons subies. Reste qu'on ne vous dira jamais assez de ne pas foncer tête baissée: exigez vos données, faites-en bon usage.

Suivez nos développements en continu
▸ **frc.ch/donnees**

impressum

Editeur
Fédération romande des consommateurs
Président
Christophe Barman
Secrétaire générale
Sophie Michaud Gigon
Responsable éditoriale
Laurence Julliard
Rédaction
Laurianne Altwegg
Florence Bettschart
Christophe Bruttin
Lionel Cretegny
Joy Demeulemeester
Robin Eymann
Aude Haenni
Sandra Imsand
Valérie Muster
Anne Onidi
Barbara Pfenniger
Sandra Renevey
Conception graphique
pixel-factory.ch
Mise en pages
Raul Minello
Photographe
Jean-Luc Barmaverain

Marketing
Sylvie André
Rédaction et abonnements
info@frc.ch
CP 6151, rue de Genève 17, 1002 Lausanne
TÉL. 021 331 00 90
Cotisation membre
70 fr. pour un an (y compris 10 numéros)
130 fr. pour deux ans (y compris 20 numéros)
Impression
Schoechli Impression & Communication sur papier certifié FSC.
Tiré à 30 000 exemplaires

ISSN 2235-7181

Photos de couverture: J.-L. Barmaverain (remerciements à Kiara et Bertrand) et shutterstock.com

point fort

Vie privée

Qui joue avec nos données?

Dossier réalisé par Aude Haenni, Robin Eymann, Florence Bettschart

Que se passe-t-il avec nos cartes de fidélité? Que faire du RGPD au quotidien en Suisse? Eclairage.

En mai, le consommateur fait ce qu'il lui plaît? Eh bien, en matière de protection des données, cela semble bien avoir été le cas. Les sollicitations d'entreprises diverses et variées pour obtenir le consentement explicite (ou non) de garder les informations personnelles le concernant ont inondé les boîtes e-mails. A vous de choisir qui vous autorisez à détenir certaines informations, ou d'y renoncer.

Voilà qui rend soudainement tangible la portée de termes barbares comme opt-in, RGPD dans le quotidien de nos vies. Vous avez un compte Dropbox pour échanger images et documents? Vous avez pris la navette Gatwick Express à l'automne dernier? Votre enfant de 12 ans est soudainement très inquiet de se voir sucrer son compte WhatsApp? Ce sont ces exemples et bien d'autres similaires que nous vous proposons d'aborder, toujours du point de vue du consommateur, de ses faits et gestes de chaque instant de la journée, et de son droit de protéger (ou non) sa vie privée. Depuis le 25 mai, grâce à un règlement européen, vous avez le pouvoir de décider quoi faire dans une majorité de situations. Pour les autres, il s'agit de patienter jusqu'à ce que le droit suisse fasse sa propre mue et qu'il mette entre nos mains, lui aussi, un véritable bouclier de protection.

Mieux comprendre

Que dit de nous notre vie connectée?

Pour rendre l'exploitation des données au quotidien concrète, la FRC s'est mise dans la peau d'un duo de consommateurs lambda, Alain et Zoé. Le temps d'une journée fictive et néanmoins éminemment réaliste, ils vous font voyager dans le monde des data. Extraits en sept cases d'un scénario aux forts accents de vérité.

COMMENT ÇA SE LIT

GRIS = mise en situation d'Alain et de Zoé

VERT = ce qui se passe avec leurs données

ORANGE = un événement réel

Et maintenant, avancez vos pions!

Son SwissPass dans la poche, Zoé saute dans le bus, direction le bureau.

Les applications et cartes électroniques de transport font profiter d'avantages clients liés notamment à la géolocalisation, mais récupèrent du coup de précieuses données.

Le Préposé à la protection des données a vu d'un mauvais œil que le contrôle de billets donne lieu à une collecte de données d'envergure. La jugeant disproportionnée, il a recommandé en 2016 l'effacement immédiat des informations de contrôle et l'abandon de la banque de données du SwissPass. L'actualité récente montre néanmoins l'intérêt de la géolocalisation pour indemniser des passagers.

Lexique

DONNÉES PERSONNELLES | Toutes les informations qui se rapportent à une personne identifiée ou identifiable: nom, numéro de téléphone, date de naissance, adresses postale et électronique, identifiants, numéro de compte bancaire, images de vidéosurveillance, etc.

DONNÉES SENSIBLES | Elles concernent les opinions ou activités religieuses, philosophiques, politiques, syndicales et l'origine ethnique; la sphère intime, l'état psychique, mental ou physique; les mesures d'aide sociale et les poursuites ou sanctions pénales et administratives. En principe, ces données ne peuvent être recueillies et exploitées que sur la base d'un consentement explicite.

TRAITEMENT DES DONNÉES | Regroupe toute opération, quels que soient les procédés et les moyens utilisés: collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, etc.

MÉTADONNÉES | Ces informations définissent et décrivent d'autres données. Ainsi, l'envoi d'un e-mail génère divers renseignements, dont l'adresse IP. L'ensemble des métadonnées correspond au Big Data.

PROFILAGE | Concerne toute forme de traitement automatisé de données à caractère personnel qui vise à évaluer certains aspects de quelqu'un pour analyser ou prédire sa santé, sa situation économique, ses centres d'intérêt, sa localisation, sa fiabilité, etc. **AH**

Carte de fidélité

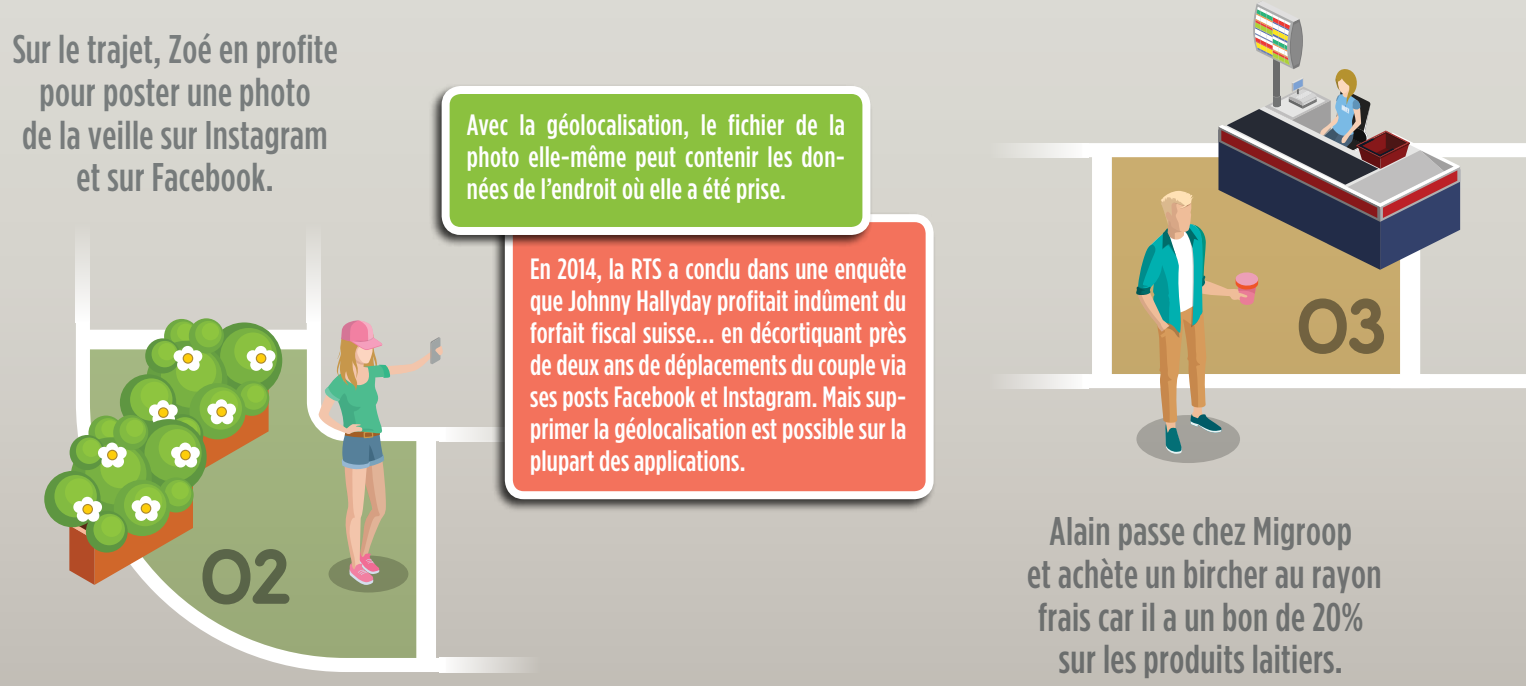
Cumulus et Supercard: au cœur de nos données

Robin Eymann

Que savent Migros et Coop de nous? Presque tout. Et les clients de ce qu'ils font des infos collectées? Presque rien.

Que disent les points Cumulus ou la Supercard des comportements d'achat et comment Migros et Coop voient-ils leurs clients? Un collaborateur de la FRC a fait valoir son droit d'accès aux données personnelles (art. 8 LPD), comme tout détenteur d'une carte de fidélité. La démarche est relativement simple: via un formulaire idoine sur le site de Migros et par courrier à Coop, avec copie de la carte d'identité. Notre «client» anonyme a reçu par pli recommandé les données le concernant entre deux et trois mois plus tard – et non dans un délai légal de 30 jours après la demande, mais moyennant avis de retard. L'intéressé «se résume» à ses coordonnées (nom, prénom, adresse, date de naissance…) et à la liste complète de ses achats, 97 pages en tout. En outre, Migros a fourni le total des dépenses effectuées depuis le début de l'adhésion au programme Cumulus ainsi que sur l'année en cours. Enfin, élément hautement intéressant, figurait dans le courrier le profil (ou «segmentation») du client.

Pour Coop, le profil se construit sur six critères: principal lieu d'achat, fréquence, préférence pour les produits durables, pour les produits bon marché, intérêt pour les rabais et pour les bons Supercard. Les critères sont assortis de variables allant de «bas» à «haut». Le système



Coop montre assez clairement dans quelles cases chacun peut figurer. Ainsi, celui qui achète des produits durables sera susceptible de recevoir des offres «Naturaplan». Notons encore que Coop enregistrait des «données relatives à la santé» (allergies alimentaires) jusqu'en 2015. Mais le Préposé fédéral à la protection des données a demandé que cesse cette collecte disproportionnée.

Une science inexacte

Le profil lié à Cumulus est plus obscur à saisir. D'abord, il n'est qu'en allemand; ensuite, le client est «trié» sur la base de trois critères: motif d'achat, prix et âge ou situation de vie (jeune, couple, parents), le tout étant qualifié par des expressions. Sous motif d'achat, notre client est – ici – «Preis/Leistung» (soit «orienté vers le rapport qualité-prix»). Côté comportement face aux prix, il est considéré comme «Premium Käufer», les produits haut de gamme (Sélection) l'attirent donc. Contradiction dans les termes? Selon la Migros, interrogé à ce propos, le fait d'avoir un profil marqué pour le haut de gamme et les prix bas s'explique: «Il se peut que nous n'ayons qu'une vision partielle des goûts du ménage, car le client n'effectue que certains achats chez nous ou ne présente pas forcément sa Cumulus. Il est aussi possible que son compte soit alimenté par différents membres du ménage, où chacun a des comportements foncièrement différents… Le marketing n'est pas une science absolue!»

La FRC a demandé quels autres critères permettaient de segmenter les gens chez Migros. Mais la transparence n'est pas de mise à Zurich: le groupe refuse de communiquer ces informations pour des questions de… «concurrence et de protection des données»! Il aurait fallu multiplier nos enquêteurs mystères pour saisir d'autres profils. Nous avons tout de même réussi à savoir que certains clients sont «Preis-affin» (affinité au prix), profilés «durable» ou «produits frais». En revanche, le fait de collecter des points avec la carte de crédit Mastercard Cumulus, l'abonnement M-Budget Mobile et des achats de pharmacie sur le site Zur Rose, ne contribuent pas à affiner le profil client.

Obtenir ses données permet au consommateur de se faire une idée sur les éléments que les coopératives retiennent, mais la transparence s'arrête là, les groupes orange ne font pas de zèle. C'est même un peu sous la contrainte qu'ils ont agi, suite à une recommandation du Préposé fédéral à la protection des données qui, en 2014-2015, a jugé que l'information sur la segmentation du client était «nécessaire à ce dernier pour se faire une idée des critères d'analyse, évaluer leur exactitude et se comporter en conséquence».

Sami Coll, sociologue et auteur d'un livre consacré à la surveillance exercée par les cartes de fidélité (*Surveiller et récompenser: les cartes de fidélité qui nous gouvernent,* Ed. Seismo, 2015), regrette qu'il ne soit pas possible de savoir concrètement comment sont utilisées les données, «il y a asymétrie de l'information: alors que le client est totalement transparent, Migros et Coop font preuve d'une grande opacité sur son utilisation». Les données que renvoient les enseignes au client qui en a fait la demande sont uniquement celles que le consommateur a fournies. On sait aujourd'hui que les technologies de type Big Data permettent une analyse extrêmement fine du profil d'une personne: déduire son orientation sexuelle, ses affinités politiques ou ses croyances religieuses. Et ces données sensibles sont bien plus problématiques que la mémorisation des tickets de caisse.

Les tickets multiplicateurs de points
▸ **frc.ch/cartes-fidelite**

Les cartes de fidélité enregistrent chaque achat et peuvent créer des profils très précis du client et de son ménage.

Grâce aux cartes de fidélité, les distributeurs savent comment pousser à l'achat: les actions sont de plus en plus personnalisées selon les intérêts de chacun. Ils savent aussi vous faire payer un «oubli»: un client Migros qui avait omis de scanner sa viande s'est fait pincer 15 jours plus tard, confondu par une vidéo de surveillance et sa carte Cumulus…

Les objets connectés dans le domaine du sport permettent d'obtenir un assistant personnel qui récolte au passage l'ensemble de notre forme physique.

Vous faites vos 10 000 pas par jour? Hop, 40 centimes d'avoirs! Si l'assuré court, marche, s'inscrit à un fitness en utilisant l'app maison de CSS, Sanitas et Swica, celles-ci offrent alors divers rabais sur les produits complémentaires. En avril dernier, le Préposé fédéral a considéré que Helsana+ allait trop loin en traitant des données de l'assurance de base.

A la pause de midi, Zoé fait une petite séance de jogging, smartphone au bras.

RGPD

Quelles conséquences pour le consommateur?

Florence Bettschart et Aude Haenni

Ce règlement est entré en vigueur en Europe le 25 mai. Il touche aussi la Suisse par ricochet. Explications.

Vous recevez des e-mails par dizaines provenant d'entreprises qui se mettent à jour. De quoi prendre conscience qu'elles se sont alignées au Règlement général sur la protection des données (RGPD). Celui-ci a de nombreuses conséquences pour les sociétés, y compris les suisses, qui doivent s'y conformer – faute de quoi, elles encourent d'importantes amendes. Il a aussi des effets pour les consommateurs. Twitter annonce d'ailleurs que «vous avez le dernier mot sur la question de savoir si nous traitons vos données personnelles et de quelle manière». Le point.

CONSENTEMENT EXPLICITE | «Nous aimerions vous envoyer des offres exclusives». Cochez oui ou non, point barre! Fini les tournures qui portent à confusion, fini les cases pré-cochées. Désormais, l'accord est explicite (on parle d'opt-in), sans équivoque, que les entreprises souhaitent vous inscrire à une newsletter, faire de la prospection commerciale, vous créer un compte fidélité, etc. Un achat devrait clairement être possible sans traitement de données, soit sans création d'un profil d'utilisateur, si cela n'est pas nécessaire à sa réalisation.

CONSENTEMENT DES MINEURS | Les risques attachés au traitement des données sont souvent complexes pour les adultes. Alors imaginez pour les enfants! Depuis l'entrée en vigueur du RGPD, le mineur de moins de 16 ans doit avoir l'autorisation de ses parents pour utiliser un réseau social, des jeux vidéo en ligne, des sites de streaming... L'application WhatsApp a par exemple récemment demandé à ses utilisateurs suisses de confirmer qu'ils avaient au moins 16 ans pour qu'ils puissent continuer à envoyer des messages. En cas de violation de cette règle, WhatsApp pourra tout simplement bloquer l'utilisation de ses services. Mais comme il reste difficile de prouver son âge d'un simple clic, la portée de cette mesure reste symbolique.

PORTABILITÉ DES DONNÉES | Données nominatives, de géolocalisation, de consommation, historique personnel, e-mails et toute autre information fournie par l'internaute pourront être récupérés chez un prestataire de service que l'on quitte et transférés gratuitement auprès du nouvel élu. Si vous désirez passer de Yahoo à Gmail, vous devriez pouvoir transférer les e-mails, ainsi que le carnet d'adresses qui y est lié. Mais ne vous réjouissez pas trop vite: en Suisse, le projet de loi – en discussion devant les Chambres fédérales – ne prévoit pas ce droit.

«PRIVACY BY DESIGN» ET «PRIVACY BY DEFAULT» | Pourquoi une application GPS voudrait-elle avoir accès à votre agenda, à vos contacts, à la caméra ou à vos sms? Ces informations n'ont aucun intérêt si ce n'est d'espionner vos données. Dorénavant, la «protection de la vie privée dès la conception» doit être intégrée dans les nouvelles applications technologiques et «la protection de la vie privée par défaut» doit permettre d'obtenir rapidement et facilement le plus haut niveau de protection possible.

RÉCLAMATION | Une société trahit la confiance des internautes d'une manière ou d'une autre? Ceux-ci pourront

Des données publiques comme celles de la Feuille d'avis officielle peuvent être croisées avec d'autres achetées (aux maisons de recouvrement p. ex.) pour définir des profils de solvabilité.

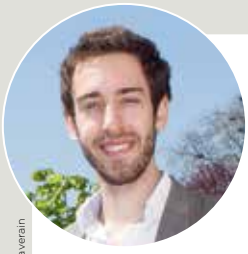
En mai 2017, le Tribunal administratif fédéral a contraint Moneyhouse à obtenir l'accord des particuliers avant de divulguer des informations personnelles. En effet, la société proposait des profils avec de nombreuses informations (réputation, situation familiale, etc.).

Pour commander un taxi, il faut télécharger l'app sur son smartphone, entrer nom, prénom, numéro de téléphone, e-mail et payer avec sa carte de crédit.

Jusqu'en 2015, Uber pistait les utilisateurs ayant un iPhone. En 2016, les employés ont affirmé pouvoir très facilement accéder aux informations personnelles des clients, y compris à l'historique des trajets. Un an après la fuite, le patron a révélé que 58 millions de données, clients et chauffeurs confondus, avaient été piratées.

Alain cherche à obtenir un crédit en ligne. Il n'a jamais été mis aux poursuites et espère que l'argent lui sera accordé.

mandater des organisations ou associations à but non lucratif pour introduire une réclamation en leurs noms, ce qui constitue une forme d'action collective. La quadrature du net – association européenne de défense des libertés numériques – a déjà mis en place, pour le 28 mai, une série de procédures collectives envers les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) qui «nous font payer leurs services avec nos libertés».



Jean-Luc Barmaverain

L'avis de l'expert

«Veillez à refuser tout ce qu'il est possible de refuser»

David Raedler, avocat, spécialiste de la protection des données et de la sphère privée

Le consommateur sera confronté à diverses pratiques, que les articles ou les services proviennent d'un marché purement indigène ou à visée internationale.

Le consommateur suisse est-il concerné par le RGPD?

Du moment que le responsable du traitement des données est Européen, oui. Il peut y avoir des cas particuliers, notamment dès lors que la commande est faite à un sous-traitant suisse d'un prestataire européen. La difficulté pour le consommateur, évidemment, est de savoir où est basé le responsable du traitement.

Cela signifie-t-il qu'il peut prétendre aux mêmes droits?

Dès le moment où le RGPD s'applique à lui, le consommateur peut prétendre aux droits qui y sont prévus. Alors que certains sont déjà prévus en droit suisse, par exemple le droit à l'effacement des données, d'autres n'existent qu'en droit européen. C'est le cas notamment du droit à la portabilité, soit le fait de faire transférer ses données de l'entreprise qu'on quitte pour celle chez laquelle on va.

Qu'en est-il si l'entreprise est suisse et que les données sont traitées dans notre pays?

Cela ne change rien pour l'instant, mais seule une minorité est concernée. La Suisse attend que la nouvelle mouture de la Loi sur la protection des données soit sous toit. Ainsi, par exemple, un vol de données n'a pas besoin d'être annoncé dans les 72 heures selon le droit suisse actuel (cas Swisscom divulgué cinq mois plus tard).

Le RGPD impose la mise à disposition d'une information claire, intelligible, accessible. Doit-on tout de même faire attention lorsque l'on coche une case?

Il faut surtout faire attention à refuser tout ce qu'il est possible de refuser. Quitte à revenir sur l'une ou l'autre décision par la suite.

Un dernier conseil?

Demandez l'accès à vos données. Cela vous permet de constater tout ce que les entreprises ont sur vous, à quel point cela va loin, et d'adapter votre comportement en conséquence. **AH**