SAPEURS POMPIERS
Ille & Vilaine

JOURNEE D'ACCUEIL ET DE RECRUTEMENT DES SAPEURS-POMPIERS VOLONTAIRES DU 25 MAI 2019

EPREUVE DE COMPREHENSION DE TEXTE
Durée : 30 minutes

DEROULEMENT DE L'EPREUVE : Ce **test** a pour objectif d'évaluer la capacité du candidat, en matière de compréhension de texte, à suivre la formation initiale de sapeur-pompier volontaire. **BAREME D'EVALUATION :** Le test est noté sur **20 points** et est composé de **10 questions** notées sur **16 points.** Grammaire et orthographe : -**0.25 point par faute** sur un total maximal de 2 points Capacité rédactionnelle : **Chaque réponse doit faire l'objet d'une phrase complète** (sujet/verbe/complément). Une réponse, même juste, ne respectant pas cette forme entraîne une déduction de 0.25 point sur un total maximal de 2 points.	**Note** **/20**

NOM : …… **Prénom** : …… **Centre d'Incendie et de Secours de** : ……	**Groupe**

QUESTIONNAIRE

Question n° 1 *(1 point)* **Qu'appelle-t-on le nouvel or noir ?**	Note **/1**
Question n° 2 *(1 point)* **Quelle problématique l'affaire Facebook/Cambridge Analytica a-t-elle soulevée ?**	Note **/1**
Question n° 3 *(2 points)* **Citez 2 objectifs du RGPD :**	Note **/2**
Question n° 4 *(2 points)* **A quoi s'exposent les entreprises qui ne respectent pas le RGPD ? Précisez votre réponse**	Note **/2**

Question n° 5 *(2 points)* **Citez au moins une critique et un risque associés aux big data selon l'auteur.**	Note **/2**
Question n° 6 *(1 point)* **Que signifie « machine learning » ?**	Note **/1**
Question n° 7 *(1 point)* **En quoi consiste le « machine learning » ?**	Note **/1**
Question n° 8 *(2 points)* **Le RGPD est aujourd'hui appliqué :** ☐ **Aux États-Unis** ☐ **En Suisse** ☐ **En France** ☐ **Au Royaume Uni** *Cocher la(les) bonne(s) réponse(s)*	Note **/2**
Question n° 9 *(2 points)* **Quelles sont les 2 principales raisons qui, selon l'auteur, ne permettent pas au RGPD de garantir une protection complète du citoyen européen ?**	Note **/2**
Question n° 10 *(2 points)* **Quelles solutions propose l'auteur pour améliorer l'utilisation des données ?**	Note **/2**
Orthographe et grammaire	Note **/2**
Capacité rédactionnelle	Note **/2**
TOTAL	Note **/20**

Avec le RGPD, la fin des dérives et des scandales ?

15 avril 2019, 20:21 CEST

Auteur : Hoareau Emilie Maître de conférences en Sciences de gestion, Systèmes d'Information, Université Grenoble Alpes

Publié par : The Conversation France.

Depuis quelques années, l'actualité est régulièrement secouée par des scandales liés à l'utilisation illicite ou abusive de données numériques. Le cas Facebook-Cambridge Analytica a particulièrement marqué les esprits. Plus que les précédentes affaires, il a mis en avant la responsabilité d'une organisation vis-à-vis des données qu'elle détient. En effet, ce ne sont pas tant les pratiques de Cambridge Analytica qui ont été dénoncées, mais bien l'incapacité du célèbre réseau social à protéger ses utilisateurs. Convoqué par les hautes instances américaines et européennes, Mark Zuckerberg a reconnu sa responsabilité dans cette affaire et s'est publiquement excusé.

Hasard du calendrier dira-t-on, le mea culpa du dirigeant de Facebook auprès des autorités européennes a eu lieu très peu de temps avant l'application du Règlement général de protection des données (RGPD). Applicable le 25 mai 2018 à l'ensemble des pays de l'Union européenne, le règlement a été en fait adopté deux ans plus tôt, après plusieurs années de négociations. Le RGPD a pour principal objectif d'encadrer la collecte et le traitement des données personnelles des citoyens européens. En ce sens, il vient renforcer les exigences envers les organisations afin de mieux protéger les consommateurs et utilisateurs de services numériques que nous sommes.

Des sanctions fortes sont prévues en cas de non-respect du règlement, puisque les amendes administratives peuvent atteindre 20 millions d'euros ou 4 % du chiffre d'affaires mondial de l'entreprise incriminée. Des montants dissuasifs que la CNIL n'hésite pas à infliger, comme le montre la condamnation récente de Google. Faut-il en conclure que les scandales de type Facebook–Cambridge Analytica feront bientôt partie du passé ? Qu'en respectant le RGPD, les organisations ne pourront plus porter atteinte aux consommateurs ? Que les citoyens européens que nous sommes sont désormais hors de toute menace ? Rien n'est moins sûr !

Le big data et ses menaces

Pour en avoir le cœur net, il suffit d'observer de près les pratiques actuelles d'utilisation des données. À l'heure du big data, la donnée est un nouvel or noir, une manne qu'il est possible de collecter et de traiter pour en retirer de la valeur. La démarche consiste principalement à identifier des schémas récurrents au sein d'une grande quantité de données. Les modèles ainsi créés sont ensuite utilisés pour prendre des décisions. À titre d'illustration, il est possible de citer le recours au Machine Learning pour la prédiction du « churn », le départ d'un client.

La « machine apprenante » est entraînée sur une grande quantité de données afin de pouvoir prédire la valeur d'une variable cible, ici la décision d'un client de ne pas renouveler son contrat. Une fois le modèle prédictif créé par apprentissage, celui-ci peut être implémenté au sein de systèmes informatiques. Il devient alors possible, à partir d'une base de données client, de déceler les signes avant-coureurs d'une résiliation de contrat et agir en conséquence, par exemple l'envoi programmé d'une offre promotionnelle. Le machine learning, tout comme d'autres techniques relatives aux big data, permet ainsi de prendre des décisions sur la base du traitement d'une grande quantité de données. Reste néanmoins un doute. Ces données, ces modèles et ces décisions ne pourraient-ils pas, d'une façon ou d'une autre, porter atteinte aux consommateurs ?

Aux USA, des voix de plus en plus nombreuses s'élèvent pour dénoncer les méfaits des pratiques liées au big data. La data scientist Cathy O'Neil parle de « weapon of math destruction » (armes de destruction mathématique) pour décrire des modèles biaisés dont les décisions amplifient les inégalités et menacent la démocratie. Car malgré l'aura d'impartialité qu'on leur prête, les modèles sont loin d'être complètement neutres. Ils peuvent contenir des erreurs ou approximations inhérentes aux données, intégrer les préjugés de leurs concepteurs, et conduire ainsi à des conclusions arbitraires et discriminatoires.

Pourtant, ces armes de destruction mathématiques sont aujourd'hui utilisées pour prendre des décisions aussi cruciales que l'acceptation d'une demande de crédit, le recrutement d'un nouvel employé ou la remise en liberté d'un prisonnier. Citons pour exemple l'outil COMPAS utilisé par les cours de justice américaine pour estimer le risque de récidive et sévèrement critiqué pour ses préconisations défavorables à la communauté afro-américaine notamment. COMPAS n'est qu'un cas parmi d'autres. Plusieurs rapports américains ont souligné les risques que représente le big data dans divers domaines : publicités ciblée visant des personnes vulnérables, exclusion d'individus jugés « à risques », imposition de tarifs plus élevés pour certaines offres de crédit ou d'assurance, filtrage informationnel qui limite l'ouverture à des idées et perspectives différentes, la liste des menaces est longue et les enjeux élevés aux États-Unis.

Avec le RGPD, sommes-nous protégés en Europe ? Plusieurs éléments incitent à en douter. En premier lieu, le RGPD s'appuie principalement sur les principes de transparence et de consentement éclairé. Les personnes sont informées des finalités et modalités de traitement des données. Elles peuvent donc prendre une décision en toute connaissance de cause : accepter ou refuser la collecte de leurs données. Or, même avec un niveau d'informations accru, la décision est-elle réellement éclairée ? Les subtilités du big data ne sont pas nécessairement connues de tous.

Par ailleurs, ce n'est pas tant les raisons pour lesquelles les données sont utilisées qui posent problème, que la façon dont elles sont traitées. En effet, si les modèles décrits par Cathy O'Neil sèment la destruction, c'est parce qu'ils sont biaisés, conçus et alimentés par des données de mauvaise qualité et employés de façon inadéquate. Passé l'étape de collecte, le consommateur n'a que peu de recul et de moyens d'intervention sur ces aspects.

En deuxième lieu, les traitements associés au big data peuvent très bien s'effectuer sur des données qui ne sont pas à caractère personnel. L'objectif n'est pas d'atteindre un individu en particulier, mais de créer un modèle contenant des règles de décisions, à partir d'un volume immense de données. Ceci nous amène à un troisième point : Les dérives du big data ne relèvent pas uniquement une atteinte à la vie privée. Elles portent également sur un traitement inéquitable des personnes. Il s'agit de discrimination. Avec ces modèles, les données et les algorithmes, la discrimination peut prendre une nouvelle ampleur. Elle est en mesure de devenir massive, automatisée, difficile à constater car ce n'est plus un être humain qui prend la décision, mais une machine aux processus opaques, une « boîte noire » qui décide sans fournir aucune explication.

Le problème est-il bien posé ?

Les scandales concernant l'utilisation des données renvoient principalement aux problématiques de la vie privée. À ces menaces pressantes, le RGPD répond en se focalisant sur un type particulier de données : les données à caractère personnel. Pourtant, des données anonymes ou rendues anonymes, ou des données personnelles collectées avec le consentement peuvent très bien causer des atteintes importantes par leur effet discriminatoire. À trop se focaliser sur la vie privée et les données personnelles, ne risque-t-on pas d'éluder les autres dangers ?

La problématique posée par les données n'est-elle pas finalement ailleurs ? Ce qui induit un risque pour le consommateur, ce ne serait pas seulement le type de données, données personnelles ou non, mais également la façon dont elles sont utilisées. Si c'est effectivement le cas, un cadre juridique centré sur les données personnelles ne pourrait suffire. Pour gérer les données, il serait plus pertinent de réguler les pratiques, les technologies, les méthodes et les outils employés par les entreprises. À ce niveau, le droit peine à suivre tant les évolutions sont rapides. Comment procéder pour protéger les citoyens sans freiner l'innovation ?

L'une des pistes envisageables serait de poser une réflexion éthique concernant l'utilisation des données. Plus exactement que les organisations prennent conscience que tout ce qui est possible n'est pas forcément souhaitable, que la façon dont elles gèrent les données peut être guidée par des valeurs connues et partagées. Ces réflexions seront probablement indispensables dans les années qui viennent pour gagner ou du moins retrouver la confiance des consommateurs. Elles demandent pourtant un changement de posture difficile aux organisations : ne plus reconnaître leurs torts après avoir été prises sur le fait, comme l'a fait Mark Zuckerberg, mais prendre leur responsabilité une fois pour toutes et tenir ensuite leur engagement. Il semble donc que la route soit encore longue pour que l'affaire Facebook-Cambridge Analytica fasse définitivement partie du passé.