GDPR: les entreprises toujours dans le flou… **par Brigitte Doucet - 08/12/2017**

L'arrivée, en mai prochain, du Règlement général européen sur la protection des données (RGPD, ou GDPR en anglais) continue de faire couler beaucoup d'encre. Chaque jour, divers observateurs regrettent l'attentisme dont font preuve les entreprises et organismes public, dénoncent le flou ou les incertitudes qui planent encore sur ce que ce nouveau règlement impliquera pour les processus des entreprises et la manière de gérer leurs données.

Une récente étude internationale commanditée par Trend Micro, société spécialisée dans les solutions de cyber-sécurité, ne va sans doute pas apaiser les esprits.

Cette enquête, menée par Opinum dans 11 pays *(voir la méthodologie en fin d'article*), révèle une perception encore largement lacunaire des implications de cette nouvelle réglementation.

En cause, notamment, ce qui est considéré comme un manque de précision dans le texte. Un exemple? L'article 32 du texte qui porte sur les mesures que les entreprises sont sensées prendre pour protéger la sécurité des données traitées. C'est plus particulièrement l'expression "état des connaissances" ("state of the art", en anglais) qui semble poser problème.

Que dit le texte? *"Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque."*

Voilà qui manque de clarté estiment les observateurs. Et l'étude de Trend Micro confirme que la formulation laisse trop de place à l'interprétation.

- 30 % des sociétés interrogées estiment que le fait d'avoir acheté une solution de sécurité auprès d'un leader du marché suffit pour être considérée comme en règle
- 26 % se disent qu'une validation de la solution par un prestataire indépendant est une garantie suffisante
- 16 % pensent que le concept d'"état des connaissances" s'applique à des produits qui… obtiennent de bonnes évaluations dans les rapports d'analystes
- 14 % interprètent "état des connaissances" comme "solutions conçues par des start-ups proposant des technologies innovantes"
- 9 % des personnes interrogées dans le cadre de cette étude se disent quant à elles incapables de donner une quelconque définition de ce que signifie "conforme à l'état des connaissances".

Rik Ferguson (Trend Micro): "Les autorités de régulation devraient clarifier davantage ce que signifie précisément "état des connaissances", de telle sorte que les entreprises ne s'exposent pas à des amendes en mai 2018."

L'étude de Trend Micro s'est aussi penchée sur l'aptitude qu'ont ou non les entreprises à se conformer aux dispositions du règlement en cas de vol, perte ou fuite de données.

Là encore, les résultats semblent préoccupants alors que, pour rappel, les sociétés interrogées ont une taille qui, en principe, devraient leur permettre de mobiliser les moyens nécessaires pour se mettre en ordre…

- 37 % des sociétés interrogées n'ont encore défini aucun protocole visant à informer les clients en cas de fuite de données
- 21 % des sociétés ont élaboré ce genre de protocole mais uniquement pour avertir les autorités ; le processus d'information aux clients concernés, lui, est encore aux abonnés absents
- de nombreuses entreprises seraient encore incapable de prendre les dispositions nécessaires pour faire respecter le droit à l'oubli d'un client; si la majorité des sociétés sondées peuvent le faire lorsqu'elles sont elles-mêmes à la source de la collecte des données client; les choses se compliquent lorsque la collecte est le fait de tiers ou de partenaires…