Faculté des Sciences & Techniques — Université de Limoges

Master 1ère année

Sécurité des Usages TIC

Examen — mai 2018

Durée : 1h30 — Tous documents autorisés

Réglementation & sécurité — 15 points

1 – L'essentiel à connaître sur le GDPR / RGPD : définition, périmètre, principes et mesures

15pts

http://www.custup.com/introduction-gdpr-rgdp/

Le GDPR (ou RGPD) est le nouveau règlement européen sur la protection des données. Il entrera en application en 2018 et impactera toutes les entreprises opérant du traitement de données à caractère personnel sur des résidents européens.

Le GDPR poursuit plusieurs objectifs ambitieux :

- Uniformiser au niveau européen la réglementation sur la protection des données.
- Responsabiliser davantage les entreprises en développant l'auto-contrôle.
- Renforcer le droit des personnes (droit à l'accès, droit à l'oubli, droit à la portabilité, etc.).

Définition et périmètre du GDPR Le GDPR « *General Data Protection Regulation* », aussi désignée sous son acronyme français RGPD « *Règlement général de protection des données* » est le nouveau texte de référence en matière de protection des données au niveau européen. Le règlement a été publié en mai 2016, après de longues années d'élaboration. Le GDPR entrera en vigueur le 25 mai 2018. Dans la mesure où il s'agit d'un règlement européen, et non pas d'une directive, le texte entrera en application directement et en même temps dans tous les Etats membres de l'Union européenne, sans transposition.

Le périmètre d'application du GDPR Les règles et obligations du GDPR s'appliquent au traitement – automatisé ou non – des données à caractère personnel. L'objectif du GDPR est de renforcer l'encadrement des pratiques en matière de collecte et d'utilisation des données à caractère personnel. La RGPD donne une définition précise des « *données à caractère personnel* » (DCP) : il s'agit de ❶« *toute information se rapportant à une personne physique identifiée ou identifiable* ». Par personne physique identifiable, il faut comprendre « *une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

Les 4 principes clés du GDPR et les mesures qui en découlent Les dispositions du GDPR s'articulent autour de 4 principes clés : le consentement, le droit des personnes, la transparence et la responsabilité.

- **Le consentement** Le GDPR renforce la notion de consentement. A partir du 25 mai 2018, le consentement des individus quant à la collecte et au traitement des données à caractère personnel les concernant devra être explicite et « *positif* »❷. Ce consentement pourra être retiré à tout moment par les individus le demandant. Les entreprises faisant du traitement de données devront, par ailleurs, être en mesure de prouver le recueil de ce consentement le cas échéant (en cas de contrôle de la CNIL).
- **La transparence** La transparence est le deuxième grand principe mis en avant par la RGPD. Il s'articule au consentement, dans la mesure où la transparence est la condition de possibilité d'un consentement explicite et éclairé. Les entreprises devront – et ce dès la phase de collecte – fournir aux individus des informations claires et sans ambiguïté sur la manière dont leurs données seront traitées.
- **Le droit des personnes** Un des principaux objectifs du GDPR est de renforcer les droits des personnes physiques. Les résidents européens se voient attribuer de nouveaux droits :
  - Un **droit d'accès facilité** pour tous les utilisateurs❸. Le responsable du traitement devra faciliter l'exercice de ce droit, par la mise en place de process et d'outils adaptés. Si la collecte s'opère sur le site internet par exemple, une solution électronique devra être prévue, si possible avec un accès à distance sécurisé.
  - Un **droit d'oubli** pour tous les utilisateurs❹. L'apport majeur de la réglementation réside dans l'extension de conditions d'exercice de ce droit. Les entreprises disposeront d'un délai réduit d'un mois, et non plus de deux mois, pour supprimer les données à la suite d'une demande. Toutes les copies et toutes les reproduction des données devront aussi être effacées.

- □ Un **droit à la limitation du traitement❺**, applicable dans quelques cas précis.
- □ Un **droit à la portabilité des données❻**. Il s'agit d'un nouveau droit qui permet à une personne de récupérer les données qu'elle a fournies, sous une forme aisément réutilisable et, le cas échéant, de les transférer à un tiers (en cas de changement de fournisseur de services par exemple).

- **La responsabilité (accountability)** Le GDPR vise à responsabiliser davantage les entreprises dans leur traitement des données à caractère personnel. Cela se traduit par :
  - ▷ L'obligation faite aux entreprises de **documenter toutes les mesures et procédures** en matière de sécurité des DCP. Les entreprises devront être en mesure de démontrer leur conformité avec la réglementation en cas de contrôle de la CNIL. Cette mesure se traduit par l'obligation de tenue d'un registre des traitements ❼. Ce registre permettra de constituer une base de données des traitements, mais pourra aussi servir à centraliser et à suivre toutes les démarches de conformité mises en œuvre par l'entreprise.
  - ▷ Le **renforcement des mesures de sécurité** ❽. Les entreprises sont responsables de la sécurité des données qu'elles traitent et doivent mettre en place les mesures adéquates pour la garantir (pseudonymisation des données, analyses d'impact, tests d'intrusion…).
  - ▷ La **notification en cas de faille de sécurité** « *data breach* » ❾. Les entreprises auront pour obligation de mettre en place des actions en cas de violation de sécurité entraînant la destruction, la perte, l'altération ou la divulgation non autorisée de DCP. En cas de faille de sécurité, l'entreprise devra la notifier à l'autorité de régulation compétente (en France, la CNIL) dans un délai de 72h. Les personnes physiques concernées devront être informées « *dans les meilleurs délais* » si la faille ou la violation de données comporte un risque élevé pour les droits et libertés.

Questions :

Pour chaque question vous proposerez une procédure et les éléments cryptographiques à utiliser.

a. Comment peut-on garantir l'unicité d'une personne dans les DCPs ❶ ? Comment regrouper les données entre elles ? Comment éviter que des informations d'un individu soient, par erreur, associées à un autre individu ?
Faites une analyse DICP du serveur mettant en œuvre cet accès. *(2pts)*

b. Comment peut-on « *prouver* » l'obtention du consentement ❷ ? *(2pts)*

c. Comment empêcher un utilisateur d'avoir accès à des données ❸ qui ne sont pas les siennes ? *(2pts)*

d. Pouvez vous proposer une solution cryptographique permettant de limiter l'accès aux données de l'utilisateur ❹ et qui pourrait automatiquement en bloquer l'accès si l'utilisateur le décide ? *(2pts)*

e. S'il semble difficile de réduire l'utilisation des données par un tiers ❺, est-ce qu'il serait possible de découvrir si une donnée à été utilisée en dehors de l'entreprise initiale ? *On considérera que les données peuvent correspondrent à des informations multimédia comme une photo ou une vidéo*. *(1pt)*

f. Faites une analyse DICP du serveur mettant en œuvre ce registre ❼. Vous indiquerez des risques et des profils d'attaquants. *(2pts)*

g. Comment l'entreprise peut réaliser cette étape ❽ et assurer aux utilisateurs que cette étape est bien faite ? *(1pt)*

h. Quel canal d'information ❾ existant pourrait être utilisé pour informer et donner un niveau de criticité ? *(1pt)*

i. Discutez si l'utilisation d'une « *carte nationale d'identité électronique* » basée sur une PKI fournirait une solution aux différents problèmes évoquées ou si au contraire elle interdirait certains points du RGPD. *(2pts)*

▬▬▬ Protocoles sécurisés – 5 points

2 – 2pts

a. Expliquez comment, lors d'une connexion sécurisée sur un site Web, la confiance s'établit depuis le navigateur vers le serveur. *(1pt)*

b. Est-ce que cette confiance peut être trahie et comment y remédier ? *(1pt)*

3 – 3pts Expliquez de manière détaillée comment est assuré le bon fonctionnement du protocole Kerberos :

a. $A \rightarrow S : A, B$

b. $S \rightarrow A : \{T_S, L, K_{AB}, B, \{T_S, L, K_{AB}, A\}K_{BS}\}K_{AS}$

c. $A \rightarrow B : \{T_S, L, K_{AB}, A\}K_{BS}, \{A, T_A\}K_{AB}$

d. $B \rightarrow A : \{T_A + 1\}K_{AB}$

Vous détaillerez les différents éléments et ce qu'ils apportent/garantissent.