Les acteurs en matière de protection des données: critères de qualification & enjeux

Commission ouverte innovation, numérique et audiovisuel du Barreau de Paris - 8 juin 2023

Anne-Cécile Colas, Group DPO

Remarques générales

- Les notions de responsable du traitement (« RT ») et de sous-traitant (« ST »), sont des **notions dites « fonctionnelles »** en ce qu'elles visent à répartir les **responsabilités** en fonction des **rôles réels joués par les parties**.

- La responsabilité du traitement peut être **définie par la loi** ou encore découler d'une **analyse des éléments ou circonstances factuels de l'espèce.**

- Certaines activités de traitement peuvent être considérées comme étant **naturellement liées au rôle d'une entité** (un employeur vis-à-vis de ses collaborateurs, un éditeur envers ses abonnés ou une association à l'égard de ses membres ou encore du fait d'une expertise professionnelle).

- Une **requalification** peut être effectuée par les autorités de contrôle ou par un juge.

- Le RGPD consacre une **logique de responsabilisation** de tous les acteurs impliqués dans le traitement des données personnelles. Il impose des obligations spécifiques aux sous-traitants qui doivent notamment assister les responsables de traitement dans leur démarche permanente de mise en conformité de leurs traitements.

Qui sont les RT et les ST?

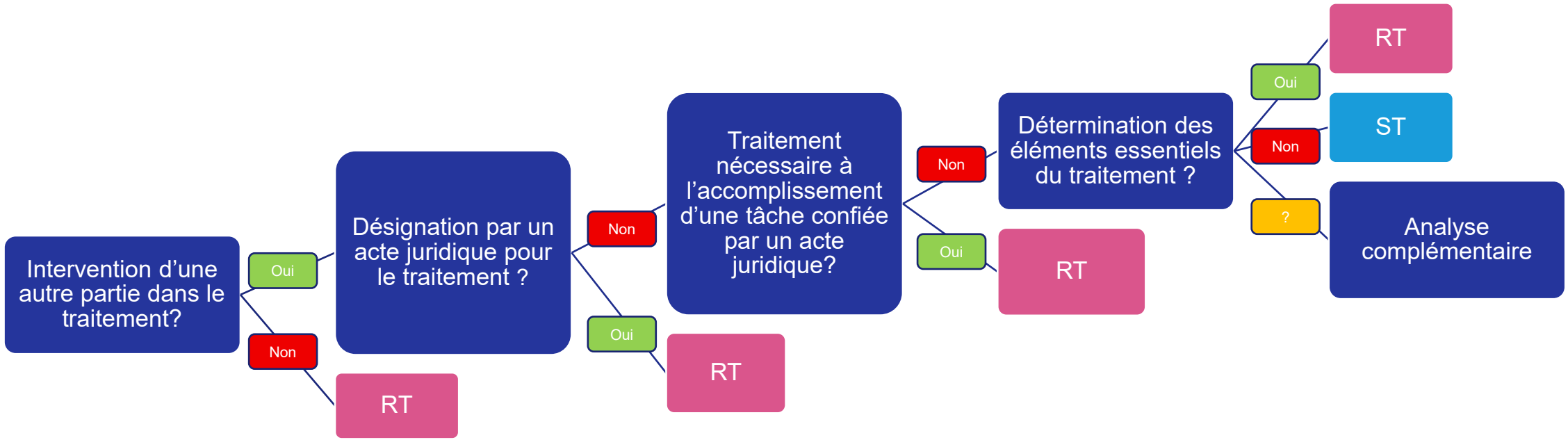
- **Article 4 du RGPD**:

> 7) «responsable du traitement», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;
>
> 8) «sous-traitant», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

- **En pratique**, il s'agit généralement de **l'organisation en tant que telle** qui fait office de RT ou ST.

- Lignes directrices 07/2020 du CEPD concernant les notions de RT et de ST :
  - Un RT décide de certains **éléments essentiels du traitement** (finalités, données collectées et traitées, catégories de personnes concernées, communication des données traitées et leurs destinataires, durée de conservation des données).
  - Un RT détermine les **finalités et les moyens du traitement, à savoir le pourquoi et le comment de ce dernier**. Le Groupe de l'Article 29 avait ajouté parmi les critères **degré d'influence et degré de précision (marge de manœuvre) sur le « pourquoi » et le « comment ».**
  - Certains aspects pratiques de la mise en œuvre («moyens non essentiels») peuvent être laissés à la discrétion du ST.
  - Il n'est pas nécessaire que le RT ait réellement accès aux données faisant l'objet du traitement pour être considéré comme un RT.

Arbre de décision de qualification de RT ou ST



Analyse complémentaire au soutien de la décision de qualification

Responsable de traitement (RT)

- Le RT **tire un avantage du traitement** ou a un **intérêt** dans celui-ci (autre que la simple rémunération des services reçus d'un autre RT)
- Le RT prend des **décisions sur les personnes concernées** dans le cadre du traitement ou à la suite de celui-ci (par exemple, les personnes concernées sont ses employés)
- Le traitement concerne la **relation du RT avec les personnes concernées** en tant qu'employés, clients, membres, etc.
- Le RT dispose d'une **totale autonomie** pour décider comment les données à caractère personnel sont traitées, y compris lorsqu'il confie le traitement de données à caractère personnel à une organisation extérieure.

Sous-traitant (ST)

- Le ST traite les données à caractère personnel pour les **finalités d'un tiers et selon ses instructions détaillées.**
- Le ST ne poursuit **pas une finalité qui lui est propre** pour le traitement en dehors de son propre intérêt commercial à fournir des services.
- Le ST doit traiter les données à caractère personnel **pour le compte du RT.** Le ST ne doit traiter les données que selon les **instructions** du RT. Ces instructions peuvent néanmoins lui laisser une certaine marge d'appréciation quant à la manière de servir au mieux les intérêts du RT, en permettant au de choisir les moyens techniques et organisationnels les plus appropriés.

Quid de la responsabilité conjointe?

Article 26 du RGPD:

1. *Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord.*
2. *L'accord visé au paragraphe 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée.*
3. *Indépendamment des termes de l'accord visé au paragraphe 1, la personne concernée peut exercer les droits que lui confère le présent règlement à l'égard de et contre chacun des responsables du traitement.*

L'article 26 du RGPD s'applique sans distinction aux relations entre des responsables de traitement, que ceux-ci soient des sociétés tierces et ou des sociétés au sein d'un même groupe (mère et filiales). En pratique, il convient de prendre en compte **l'impact des liens entre une société mère et sa filiale** sur la notion de détermination conjointe.

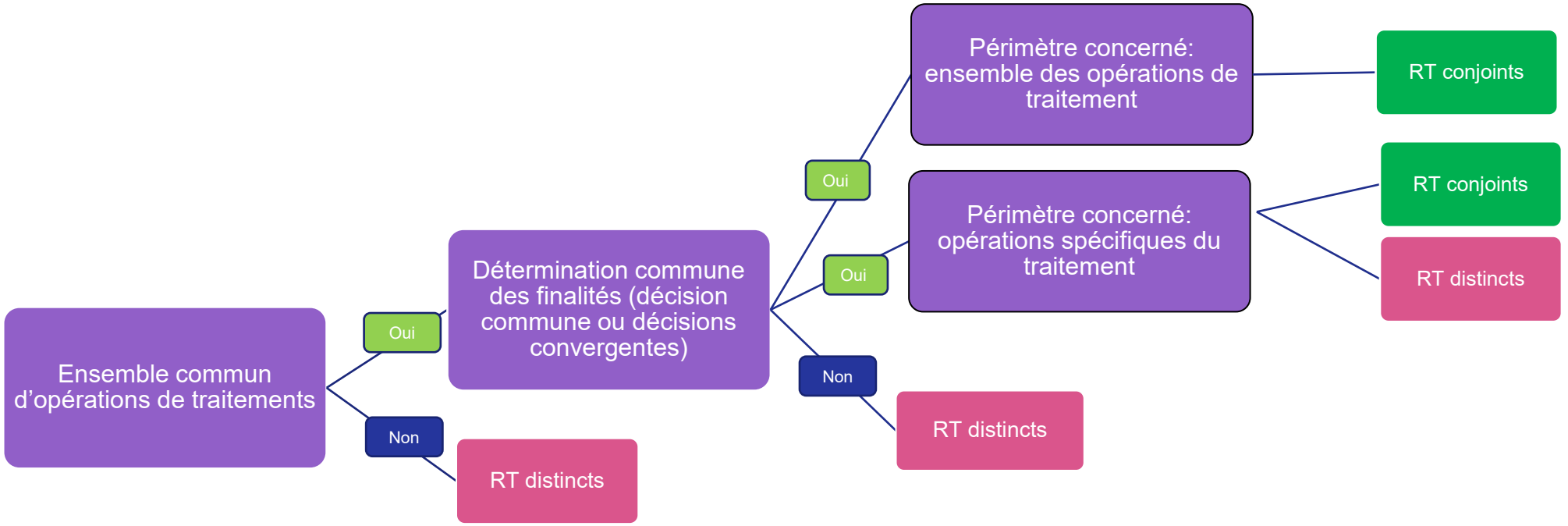
Méthodes d'identification de la responsabilité conjointe

- **Avis 1/2010 du 16 février 2010 du Groupe de l'Article 29**:
  - **Méthode de l'infrastructure commune**: détermination des éléments essentiels des moyens à utiliser
  - **Méthode de l'ensemble d'opérations** : « ensemble d'opérations » poursuivant une finalité commune ou utilisant des moyens déterminés conjointement
  - **Méthode basée sur l'origine** : mise en commun de ce que chaque RT introduit dans le système

- **Lignes directrices du CEPD du 7 novembre 2019 sur les notions de responsable du traitement, de sous-traitant et de responsabilité conjointe du traitement dans le cadre du règlement (UE) 2018/1725**
  - Lorsque les finalités et les (éléments essentiels des) moyens de l'opération de traitement sont déterminés conjointement, un **niveau « général » de complémentarité et d'unité de finalité** peut suffire à provoquer une situation de responsabilité conjointe du traitement ». On retrouve ici l'esprit de la « **méthode de l'ensemble des opérations** ».

- **Lignes directrices 07/2020 du CEPD concernant les notions de RT et de ST :**
  - Le critère essentiel pour qu'il y ait responsabilité conjointe du traitement est la **participation conjointe de deux entités ou plus dans la détermination des finalités et des moyens d'une opération de traitement** (ex.: décision commune prise par deux entités ou plus ou décisions convergentes adoptées par deux entités ou plus, lorsque les décisions se complètent et sont nécessaires à la réalisation du traitement de telle sorte qu'elles ont un effet concret sur la détermination des finalités et des moyens du traitement).

Arbre de décision - Responsabilité conjointe



Cas pratique n°1: Services de chèques cadeaux fournis à un client

Services	Qualification du prestataire	Qualification du client	Opérations de traitements
Services "Chèques cadeaux"	**ST**	**RT**	Mise à disposition de l'Interface Client à des fins de commande
	RT Conjoint	**RT Conjoint**	**Création & crédit des comptes ; Gestion des comptes bénéficiaires**
Service "Gestion" (administration, comptabilité)	**ST**	**RT**	Hébergement des données téléversées par les Clients Mise à disposition d'un site personnalisé et assistance technique

Cas pratique n°2 – SIRH unique utilisé par une société mère et ses filiales

Opérations de traitement	Qualification de la société mère	Qualification des filiales
▪ Gestion administrative des collaborateurs ▪ Gestion des mobilités ▪ Développement des carrières	RT Conjoint	RT Conjoint
▪ Enquête d'engagement groupe ▪ Analyses statistiques groupe ▪ Rapports financiers groupe	RT	N/A

Quels enjeux pour chaque qualification ?

RT

- Principes généraux de la protection des données et obligations légales de conformité, y compris l'obligation de recours à des ST qui offrent des garanties suffisantes pour mettre en œuvre des mesures techniques et organisationnelles appropriées afin que le traitement réponde à ces exigences
- Accord de traitement comprenant des clauses obligatoires (Article 28.3 du RGPD) et des informations sur le niveau de sécurité requis pour ledit traitement.

ST

- Obligations légales de conformité: mesures techniques et organisationnelles appropriées
- Obligations contractuelles sous la forme d'un accord de traitement
- Un ST viole le RGPD s'il va au-delà des instructions du RT et commence à déterminer ses propres finalités et ses propres moyens de traitement.

RT conjoints

- Double information et double moyens pour les personnes concernées d'exercer leurs droits → détermination des obligations respectives (exercice des droits des personnes
- Répartition des rôles et responsabilités sous la forme d'une convention
- Obligations à l'égard des autorités chargées de la protection des données

Merci pour votre attention