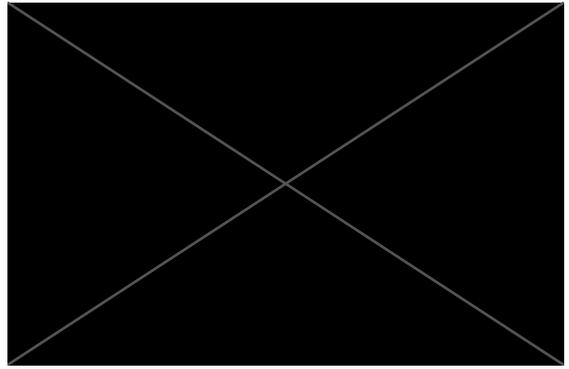




**UNIVERSITÉ  
DE GENÈVE**

**FACULTÉ DE DROIT**



**Equipements VR et protection des données sous l'angle de la nLPD**

Travail de rédaction juridique – droit et numérique

Professeur responsable : Prof. Yaniv BENHAMOU

Date de dépôt : 16 décembre 2022

Année académique 2022-2023

# Table des matières

<b>TABLE DES ABRÉVIATIONS .....</b>	<b>2</b>
<b>I. INTRODUCTION.....</b>	<b>3</b>
<b>II. L'APPLICATION DE LA nLPD AUX ÉQUIPEMENTS VR .....</b>	<b>3</b>
1. Champ d'application personnel .....	3
2. Champ d'application matériel .....	3
2.1. Traitement .....	3
2.2. Données personnelles .....	4
2.3. Personne privée .....	4
3. Champ d'application territorial .....	5
<b>III. UN TRAITEMENT DE DONNÉES LICITE .....</b>	<b>5</b>
1. Bonne foi .....	5
2. Proportionnalité .....	6
3. Finalité .....	6
4. Reconnaissabilité .....	7
<b>IV. MOTIFS JUSTIFICATIFS .....</b>	<b>8</b>
1. Consentement .....	9
1.1. Consentement libre .....	9
1.2. Consentement éclairé.....	9
1.3. Consentement spécifique .....	10
1.4. Consentement exprès .....	10
2. Intérêt privé prépondérant .....	11
<b>V. CONCLUSION .....</b>	<b>12</b>
<b>BIBLIOGRAPHIE .....</b>	<b>13</b>
<b>TABLE DES ÉQUIVALENCES .....</b>	<b>17</b>

## Table des abréviations

<b>al.</b>	alinéa
<b>art.</b>	article
<b>ATF</b>	Arrêt du Tribunal fédéral
<b>ATAF</b>	Arrêt du Tribunal administratif fédéral
<b>BSK</b>	Basler Kommentar
<b>consid.</b>	considérant
<b>CC</b>	Code civil suisse du 10 décembre 1907
<b>cf.</b>	<i>confer</i> (se référer à)
<b>ch.</b>	chiffre
<b>édit.</b>	éditeur(s)
<b>G29</b>	Groupe de travail « article 29 »
<b>LPD</b>	Loi fédérale sur la protection des données
<b>lit.</b>	littera
<b>MPT</b>	Meta Platforms Technologies
<b>nb.</b>	<i>Nota bene</i> (remarque)
<b>p./pp.</b>	page/pages
<b>PF PDT</b>	Préposé fédéral à la protection des données et à la transparence
<b>nLPD</b>	nouvelle loi fédérale sur la protection des données du 25 septembre 2020
<b>RS</b>	Recueil systématique du droit fédéral
<b>RGPD</b>	Règlement général sur la protection des données
<b>s./ss</b>	et suivant/s
<b>SHK</b>	Stämpflis Handkommentar
<b>VR</b>	Réalité virtuelle

## I. Introduction

La réalité virtuelle (VR) permet, grâce à un casque de réalité virtuelle, de simuler la présence physique de l'utilisateur dans un endroit n'existant pas physiquement. Le panier d'achat, les sites consultés, les jeux utilisés, pendant combien de temps et à quelles fréquences, sont des données qui peuvent être collectées lors de l'utilisation d'un casque VR<sup>1</sup>. Au vu du potentiel que présente la VR, il est légitime de craindre le développement de profils d'utilisateur et leur utilisation à des fins commerciales, sans que l'utilisateur n'en soit vraiment conscient. Or, il s'agit de données sensibles qui ne peuvent être récoltées que sous certaines conditions, ce que nous examinerons plus loin. Ce travail cherchera donc à déterminer si le cadre juridique posé par la nouvelle loi fédérale du 25 septembre 2020 sur la protection des données (Loi sur la protection des données, nLPD)<sup>2</sup> est suffisant pour protéger les données sensibles des utilisateurs de casques de réalité virtuelle. Le sujet étant relativement large, nous avons décidé de le restreindre au cas de Meta et de leurs casques Meta Quest et Meta Quest Pro.

Nous commencerons par examiner l'applicabilité de la nLPD (II). Nous analyserons ensuite si le traitement de données provenant de l'utilisation d'équipements VR est licite (III). S'il s'avère que le traitement est illicite, nous examinerons s'il peut néanmoins être justifié (IV).

## II. L'application de la nLPD aux équipements VR

### 1. Champ d'application personnel

La LPD en vigueur aujourd'hui protège les données des personnes physiques et morales (art.2 al.1 LPD). La nLPD, quant à elle, ne protège que les données de personnes physiques (art.2 al.1 nLPD), le Conseil fédéral ayant estimé que d'autres lois prévoient déjà une protection adéquate des données des personnes morales<sup>3</sup>, ce qui permet ainsi à la Suisse de s'aligner à l'Union Européenne qui ne prévoit pas une telle protection dans le Règlement général sur la protection des données (RGPD)<sup>4</sup>.

### 2. Champ d'application matériel

La nLPD porte sur le traitement (2.1.) de données personnelles de personnes physiques (2.2.) effectué par des personnes privées (2.3.) (art.2 al.1 lit.a nLPD)<sup>5</sup>. L'art.2 al.2 nLPD prévoit trois exceptions au champ d'application matériel, cependant aucune n'entrent en considération ici.

#### 2.1. Traitement

Le traitement, défini à l'art.5 lit.d nLPD, consiste en « toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés [...] ». Ce large champ d'application matériel s'explique par la volonté du législateur de couvrir tous types de

---

<sup>1</sup> META, Politique de confidentialité supplémentaires MPT, I. Quelles informations recueillons-nous ?, <https://bit.ly/3W6wrNC>.

<sup>2</sup> RS 235.1.

<sup>3</sup> Message du Conseil fédéral concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, 15 septembre 2017, FF 2017 p. 6565 ss, p.6595.

<sup>4</sup> Règlement n°2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO n° L 119 du 4 mai 2016, p.1.

<sup>5</sup> *Nb.* Nous ne traiterons pas de la 2<sup>e</sup> hypothèse prévue à l'art.2 al.1 lit.b nLPD concernant le traitement effectué par des organes fédéraux faute de pertinence en lien avec ce travail.

traitements de données afin d'éviter d'éventuels abus<sup>6</sup>. Dans notre cas d'espèce, la simple collecte de données des casques VR constitue déjà un traitement, même si ces données sont uniquement conservées dans le casque.

## 2.2. Données personnelles

Les données personnelles sont « toutes les informations se rapportant à une personne physique identifiée ou identifiable » (art.5 lit.a nLPD). La loi se veut très large, puisqu'il suffit que l'information ait un contenu informatif à propos d'une personne physique<sup>7</sup>. En d'autres termes, seules les données purement factuelles, celles qui sont immuables quel que soit le destinataire ou le propriétaire de la donnée (telle que la distance entre la terre et la lune) sont exclues du champ d'application matériel de la nLPD<sup>8</sup>. La référence à une personne physique est directe lorsque l'information se rapporte directement à une personne<sup>9</sup>. La référence est indirecte quand l'information ne se rapporte pas à une personne, mais que, selon le contexte ou en combinant d'autres informations, il est possible d'obtenir des renseignements sur une personne<sup>10</sup>. C'est la finalité de l'information, la manière dont elle est utilisée, qui est alors déterminante<sup>11</sup>. Par exemple, Meta collecte des informations concernant les événements de réalité virtuelle auxquels l'utilisateur participe<sup>12</sup>. L'information se rapporte à l'évènement, mais en la combinant avec le nom d'utilisateur, Meta sait que la personne y a participé. Selon MEIER, à défaut de finalité, le résultat de l'information peut alors avoir un impact sur la personne<sup>13</sup>. Ainsi, lorsque Meta collecte des statistiques sur les jeux VR, les informations collectées servent à améliorer le jeu mais aussi à déterminer la manière dont l'utilisateur utilise ce jeu. En définitive, presque toutes les données peuvent devenir des données personnelles si elles sont combinées entre elles, ce qui ressort de l'expression « toutes les informations » de l'art.5 lit.a nLPD<sup>14</sup>.

Concernant la notion de personne physique **identifiée** ou **identifiable**, une personne est identifiée lorsqu'il n'y a aucun doute sur son identité, comme les empreintes digitales. Une personne est identifiable quand elle n'est pas mentionnée directement mais qu'il est possible de remonter à elle par combinaison d'informations. S'il n'est pas possible d'identifier la personne, alors il ne s'agit pas de données personnelles<sup>15</sup>. En résumé, l'identifiabilité d'une personne est la limite pour qualifier une information de donnée personnelle au sens de l'art.5 lit.a nLPD<sup>16</sup>. À titre d'exemple, un pseudonyme utilisé pour jouer à des jeux ne permet pas de remonter à la personne, sauf en combinant cette information avec l'adresse e-mail à laquelle le compte est lié.

## 2.3. Personne privée

L'auteur du traitement, appelé responsable de traitement par la nLPD, est « la personne privée [...] qui détermine les finalités et les moyens du traitement de données personnelles » (art.5 lit.j nLPD). Il peut s'agir d'une personne physique ou morale tant que les données sont traitées à

---

<sup>6</sup> BSK DSG–MAURER-LAMBROU/KUNZ, DSG 2 N 3.

<sup>7</sup> SHK DSG–RUDIN, DSG 3 N 4 ; DE TERWANGNE, p. 57 ; MEIER, N 424 ; ATF 136 II 508 consid. 3.2.

<sup>8</sup> BSK DSG–BLECHTA, DSG 3 N 6 ; MEIER, N 422 SS.

<sup>9</sup> MEIER, N 425 ; SHK DSG–RUDIN, DSG 3 N 7.

<sup>10</sup> MEIER, N 426.

<sup>11</sup> *Idem*.

<sup>12</sup> META, Politique de confidentialité supplémentaire MPT, I. Quelles informations recueillons-nous ?, Activité du Produit MPT, <https://bit.ly/3W6wrNC>.

<sup>13</sup> MEIER, N 427.

<sup>14</sup> BSK DSG–BLECHTA, DSG 3 N 7 *in fine*.

<sup>15</sup> MEIER, N 431 SS.

<sup>16</sup> BSK DSG–BLECHTA, DSG 3 N 10 ; SHK DSG–RUDIN, DSG 3 N 10.

l'occasion d'une relation de droit privé, tel un contrat. C'est donc « [l]a nature juridique de l'activité occasionnant le traitement [qui est] déterminante »<sup>17</sup>. Dans le cas d'espèce, la distinction entre droit public et privé ne pose pas de problème puisque la relation entre Meta (personne morale) et l'utilisateur du casque VR repose sur une base contractuelle.

### 3. Champ d'application territorial

Le champ d'application territorial est prévu à l'art.3 nLPD, qui dispose que la nLPD « [...] s'applique aux états de fait qui déploient des effets en Suisse, même s'ils se sont produits à l'étranger » (art.3 nLPD). À ce propos, ROSENTHAL et STUDER précisent qu'un état de fait déploie des effets en Suisse lorsqu'il risque d'y avoir, ou qu'il y a, une atteinte à la personnalité d'une personne en Suisse<sup>18</sup>. De plus, il suffit qu'un seul événement se passe en Suisse pour déclencher l'application de la loi (comme la collecte de données). La nLPD a donc un effet extraterritorial puisqu'il suffit d'une atteinte, même hypothétique, à la personnalité, ou qu'une partie des faits se passent en Suisse, pour que la nLPD s'applique<sup>19</sup>. En l'espèce, la nLPD est bien applicable aux équipements VR, puisque le simple fait de porter un casque VR (ce qui engendre automatiquement une collecte de données) en Suisse déclenche l'application de la loi, même si ces données sont ensuite traitées à l'étranger.

## III. Un traitement de données licite

Le traitement de données est toujours possible sauf s'il porte atteinte à la personnalité de la personne concernée, ce qui est notamment le cas lorsque le traitement viole les principes prévus à l'art.6 nLPD (art.30 al.1 et 2 lit.a nLPD). Il convient de préciser que seulement quatre des sept principes énoncés à l'art.6 nLPD ne seront analysés dans ce travail, les autres n'étant pas pertinents dans notre cas d'espèce<sup>20</sup>.

### 1. Bonne foi (art.6 al.2 nLPD)

Selon le Préposé fédéral à la protection des données et à la transparence (PFPDT), ce principe « signifie que le traitement de données a été effectué de manière reconnaissable pour la personne concernée »<sup>21</sup>. Il s'agit d'un principe général qu'il convient de mettre en relation avec d'autres principes (comme celui de la reconnaissabilité également mentionné dans la définition du PFPDT). Le principe de transparence, qui dicte que la personne doit être informée de la collecte ou du traitement, découle de la bonne foi mais également du principe de reconnaissabilité (art.6 al.3 nLPD)<sup>22</sup>. Il convient de tracer une limite entre la bonne foi et la proportionnalité. Selon MEIER, si le responsable de traitement a l'obligation de détruire les données collectées mais ne le fait pas, il viole le principe de la bonne foi. Au contraire, il y a violation du principe de proportionnalité si, malgré l'absence d'obligation de détruire la donnée, le responsable de traitement garde cette donnée alors même qu'il n'en a plus besoin<sup>23</sup>. Enfin, celui qui laisse croire que toutes les données sont obligatoires alors que certaines sont facultatives viole également le principe de la bonne foi<sup>24</sup>. En l'espèce, Meta énonce bien collecter et traiter des

---

<sup>17</sup> MEIER, N 361.

<sup>18</sup> ROSENTHAL/STUDER, N 88 *in fine*.

<sup>19</sup> *Idem*, N 89.

<sup>20</sup> *Nb.* Bien que le consentement soit mentionné avec les autres principes (art.6 al.7 nLPD), il n'en n'est pas un, c'est pourquoi nous n'en parlerons que lorsque nous examinerons les motifs justificatifs, *cf.* MEIER, N 823.

<sup>21</sup> PFPDT, traitement des données personnelles dans le secteur privé, p. 4.

<sup>22</sup> MEIER, N 649.

<sup>23</sup> MEIER, N 655.

<sup>24</sup> PFPDT, traitement des données personnelles dans le secteur privé, p.4.

données personnelles liées à l'utilisation des casques VR. De plus, presque tous les types d'utilisation des casques et de leurs fonctionnalités possèdent leur propre page d'avis de confidentialité<sup>25</sup>.

## 2. Proportionnalité (art.6 al.2 nLPD)

Ce principe est composé de 4 volets que nous détaillerons ci-dessous. Premièrement, le traitement doit respecter la règle de **l'aptitude**, il doit être apte à atteindre le but visé<sup>26</sup>. Par exemple, si le but est de fournir les Produits Meta Platforms Technologies (Produits MPT) ainsi que leurs fonctionnalités, la collecte de données relatives à la réussite ou à l'échec de fonctionnalités spécifiques est apte à atteindre le but visé. Cependant, nous ne voyons pas en quoi la collecte de données concernant le contenu créé par l'utilisateur est apte à atteindre ce but<sup>27</sup>.

Deuxièmement, le traitement doit être **nécessaire**, c'est-à-dire qu'entre plusieurs moyens aptes à atteindre le but visé, il faut choisir le moins intrusif et seules les données nécessaires pour atteindre le but visé doivent être collectées<sup>28</sup>. Ainsi, pour reprendre l'exemple ci-dessus, la collecte de données concernant le contenu créé par l'utilisateur n'est pas nécessaire selon nous, puisque la non-collecte n'empêcherait pas la fourniture des Produits MPT ou de leurs fonctionnalités.

Troisièmement, les données doivent être détruites ou anonymisées dès qu'elles ne sont plus nécessaires au but visé. Il s'agit du principe de la **limitation de la conservation**. Bien qu'étant expressément prévu à l'art.6 al.4 nLPD, ce principe découle toutefois de la proportionnalité<sup>29</sup>. *In casu*, dans sa politique de confidentialité relative au suivi des yeux, Meta précise que « les données envoyées vers nos serveurs pour y être stockées sont dissociées [du compte d'utilisateur du casque] lorsque nous n'en avons plus besoin pour assurer notre service ou améliorer la fonctionnalité de suivi des yeux »<sup>30</sup>. Cette condition est donc bien respectée.

Enfin, le traitement doit respecter la **proportionnalité stricto sensu**, c'est-à-dire que l'atteinte à la personnalité résultant du traitement doit être raisonnablement exigible du point de vue de l'utilisateur<sup>31</sup>. Ce qui revient à procéder à une pesée des intérêts en présence<sup>32</sup>. Par exemple, Si le but recherché est de vérifier que l'utilisateur est en âge d'utiliser le casque, l'atteinte subie par l'obligation de renseigner sa date de naissance est donc raisonnablement exigible.

## 3. Finalité (art.6 al.3 nLPD)

L'art.6 al.3 nLPD prévoit que « les données personnelles ne peuvent être collectées que pour des finalités déterminées [...] et doivent être traitées ultérieurement de manière compatible avec ces finalités ». Selon la doctrine le principe de finalité est divisé en deux sous-principes, celui de **détermination du but** et celui **d'immutabilité du but**<sup>33</sup>.

---

<sup>25</sup> Par exemple : META, Suivi des mains, <https://bit.ly/3VO7HtU>.

<sup>26</sup> MEIER, N 665.

<sup>27</sup> META, Bases légales, finalité : fournir les Produits MPT, y compris leurs fonctionnalités, <https://bit.ly/3ULHwmf>.

<sup>28</sup> Appelé principe de minimisation cf. MEIER, N 633 et FF 2017 p. 6644 ; PRAZ, N 12.

<sup>29</sup> FF 2017 p. 6645 ; ROSENTHAL/STUDER, N 34.

<sup>30</sup> META, Suivi des yeux, Quelles données sont recueillies, Fonction de suivi des yeux, <https://bit.ly/3VMb58I>.

<sup>31</sup> ROSENTHAL/STUDER, N 34 ; ATF 138 II 346, consid. 9.2.

<sup>32</sup> MEIER, N 665 s ; FF 2017 p. 6644.

<sup>33</sup> MEIER, N 722 ; BSK DSG–MAURER-LAMBROU/STEINER, DSG 4 N 13.

Le premier sous-principe commande que les données ne soient traitées que dans un but déterminé, ce qui, selon le Conseil fédéral, est notamment le cas lorsque la personne concernée est informée du but au plus tard lors de la collecte<sup>34</sup>. Il est donc interdit de collecter des données dans un but indéterminé ou imprécis. La finalité du traitement peut toutefois être implicite si elle ressort clairement des circonstances et si elle est reconnaissable par la personne concernée<sup>35</sup>. En l'espèce, bien que Meta énonce clairement toutes les finalités pour lesquelles les données sont collectées<sup>36</sup>, le processus pour le savoir est compliqué, mais ceci sera développé plus loin lors de l'analyse du principe de reconnaissabilité. Un autre problème peut être soulevé quant au lien entre les données collectées et leur finalité. Ainsi, si l'utilisateur active la fonction « suivi des yeux » et décide de partager des données supplémentaires à Meta, ce dernier prévoit que « d'autres données concernant [l']utilisation du casque (y compris du suivi des yeux) [...] » sont collectées afin de personnaliser l'expérience de l'utilisateur et d'améliorer Meta Quest<sup>37</sup>. Il s'agit donc de finalité très vague, car « personnaliser l'expérience » peut aussi comprendre l'envoi de contenu commercial personnalisé<sup>38</sup>. Il y a donc, selon nous, un problème quant à la détermination précises des finalités invoquées par Meta et l'utilisateur ne peut pas savoir exactement ce qu'il advient de ses données<sup>39</sup>.

Le sous-principe **d'immutabilité du but** impose que les données soient toujours traitées conformément aux finalités initiales<sup>40</sup>. Ainsi, tout traitement incompatible avec la finalité initiale est égal à un nouveau traitement. En l'espèce, comme dit précédemment, Meta n'énonce pas clairement pour quelles finalités les données sont collectées, il n'est donc pas impossible que ces données soient utilisées pour des finalités différentes et incompatibles que celles énoncées à l'utilisateur. Pour prendre l'exemple du suivi des yeux, l'utilisateur ne sait pas quelles sont toutes les finalités puisque, pour avoir plus de détails, Meta renvoie l'utilisateur sur une page de confidentialité supplémentaire qui ne contient aucune information spécifique au suivi des yeux mais concerne l'ensemble de l'utilisation du casque Meta Quest Pro<sup>41</sup>.

#### 4. Reconnaissabilité (art.6 al.3 nLPD)

L'art.6 al.3 nLPD exige que la collecte des données et la finalité de leur traitement soit reconnaissable pour la personne concernée. Il convient de distinguer le principe de reconnaissabilité du devoir d'information qui incombe au responsable du traitement (art.19 nLPD). Alors que la violation du premier fait présumer l'illicéité du traitement (art.30 al.2 lit.a nLPD), la violation du second est susceptible d'une sanction pénale (art.60 nLPD)<sup>42</sup>. Selon ROSENTHAL/STUDER, cela s'explique par le fait que l'art.19 nLPD est une disposition de droit public dont la violation ne peut entraîner une atteinte à la personnalité. Ils ajoutent que le devoir d'informer « garantit qu'une personne concernée ait accès à des informations *supplémentaires* sur le traitement des données si elle y est intéressée, tandis que l'art. 6 nLPD garantit une « transparence de base » qui doit bénéficier [...] à toutes les personnes concernées »<sup>43</sup>. Toutefois,

---

<sup>34</sup> FF 2017 p. 6644.

<sup>35</sup> SHK DSG–BAERISWYL, DSG 4 N 43.

<sup>36</sup> META, Bases légales, <https://bit.ly/3ULHwmf>.

<sup>37</sup> META, Suivi des yeux, Quelles données sont recueillies, Fonction de suivi des yeux, <https://bit.ly/3VMb58I>.

<sup>38</sup> META, Politique de confidentialité supplémentaires MPT, II. Comment utilisons-nous vos informations ?, Pour proposer des fonctions sociales, personnaliser et promouvoir le contenu, <https://bit.ly/3W6wrNC>.

<sup>39</sup> SHK DSG–BAERISWYL, DSG 4 N 43 *in fine* ; CHARLET, p. 86.

<sup>40</sup> FF 2017 p. 6645 ; MEIER, N 725.

<sup>41</sup> Cf. META, Suivi des yeux, Quelles données sont recueillies, Fonction de suivi des yeux, <https://bit.ly/3VMb58I> lorsque l'on clique sur « en savoir plus » nous sommes amené sur la page suivante : <https://bit.ly/3HrDYCB>.

<sup>42</sup> MEIER, N 701.

<sup>43</sup> ROSENTHAL/STUDER, N 92.

le principe de reconnaissabilité est étroitement lié au principe de la bonne foi (*cf.* III. 1.1.) puisque tous deux exigent un traitement transparent des données. Or, selon les circonstances (telles que le type de données collectées), la bonne foi, mise en relation avec le principe de reconnaissabilité, demande que des informations supplémentaires soient reconnaissables pour la personne concernée<sup>44</sup>. En somme, le principe de reconnaissabilité s'applique au regard des circonstances du cas d'espèce et s'analyse généralement en lien avec d'autres principes. Ainsi, le traitement portant sur des données sensibles (art.5 lit.c nLPD), soit les données méritant une protection particulière du fait de l'atteinte qu'elles peuvent présenter sur la personnalité de la personne concernée, demande, en application des principes de reconnaissabilité et de la bonne foi, que des informations supplémentaires soient communiquées à la personne concernée<sup>45</sup>.

En l'espèce, la collecte de données n'est reconnaissable qu'une fois le casque acheté. Bien que le principe de finalité prévoie que la personne doit être informée du but de la collecte au plus tard lors de celle-ci, en application des principes de bonne foi et de reconnaissabilité, il est légitime de se demander si l'utilisateur ne devrait pas en être informé avant d'acheter le casque. Ainsi, Meta met en avant des fonctionnalités alléchantes comme des expressions naturelles du visage pour les avatars. Cependant, il n'est dit nulle part que Meta peut collecter des données relatives à l'utilisation de cette fonctionnalité, pour le savoir, il faut consulter leur politique de confidentialité, ce que personne ne pense à faire avant d'acheter un produit<sup>46</sup>. L'utilisateur peut choisir de ne pas utiliser toutes ces fonctionnalités, mais cela change alors totalement l'expérience. La personne se retrouve donc avec un casque qu'elle a acheté plus cher afin de profiter de ces fonctionnalités, alors qu'elle aurait pu en acheter un moins cher ne les proposant pas. Il ne lui reste plus qu'à espérer que le magasin lui rembourse son achat. De plus, des données concernant le nombre de calories brûlées lors de l'utilisation de l'application Meta Quest Move sont collectées. Il s'agit de données sensibles sur la santé au sens de l'art.5 lit.c ch.2 nLPD puisque ces données permettent de tirer des conclusions sur l'état de santé physique de l'utilisateur<sup>47</sup>. Cela demande ainsi une protection accrue et donc une application plus large des principes généraux de la nLPD<sup>48</sup>. Le PFPDT a d'ailleurs fait la même recommandation dans l'affaire PFPDT contre KSS Schaffhouse<sup>49</sup> où les clients d'un SPA n'étaient informés de la collecte de leur données biométriques qu'après leur inscription. Le PFPDT avait ainsi recommandé que les informations relatives aux traitements de données sensibles soient remises aux clients avant leur inscription<sup>50</sup>. Notre cas est similaire, puisqu'il s'agit de données sensibles et qu'aucune information n'est donnée avant d'acheter le casque. De plus, aucun personnel de magasin n'a su répondre à nos questions concernant les données qui sont connectées ni sur l'existence même d'une collecte.

#### **IV. Motifs justificatifs**

La violation de l'un des principes prévus à l'art.6 nLPD constitue une atteinte à la personnalité qui est présumée illicite (art.30 al.1 et 2 lit.a nLPD)<sup>51</sup> sauf si cela peut, notamment, être justifié par le consentement de la personne concernée (1.) ou par un intérêt privé prépondérant (2.) (art.31 al.1 nLPD).

---

<sup>44</sup> ROSENTHAL/STUDER, N 35 ; *cf.* également MEIER, N 705 et 707.

<sup>45</sup> MEIER, N 478 ; MÉTILLE, Le droit au respect de la vie privée, p. 23.

<sup>46</sup> CHARLET, p. 88.

<sup>47</sup> BSK DSG–BLECHTA, DSG 3 N 33.

<sup>48</sup> MEIER, N 480.

<sup>49</sup> ATAF 2009/44.

<sup>50</sup> ATAF 2009/44, consid 4.4.

<sup>51</sup> MEIER, N 1521.

## 1. Consentement

La validité du consentement est analysé selon l'art.6 al.6 nLPD<sup>52</sup> qui prévoit que le consentement doit être libre (1.1.), éclairé (1.2.) et spécifique (1.3.). Selon l'al.7 lit.a et b du même article, le consentement doit en outre être exprès en cas de traitement de données sensibles ou de profilage à risque élevé effectué par une personne privée (1.4.). Il convient de préciser qu'en cas de données sensibles les exigences quant à la validité du consentement sont plus élevées<sup>53</sup>.

### 1.1. Consentement libre

Selon le Groupe de travail « Article 29 » (G29)<sup>54</sup>, un consentement libre implique que la personne concernée ait le choix de ne pas consentir, ce qui n'est pas le cas si elle ne peut pas refuser le traitement sans subir de préjudice<sup>55</sup>. Il y a notamment préjudice lorsque le refus de consentir implique des désavantages comme un service de moindre qualité ou le refus du service<sup>56</sup>. Il faut cependant que le désavantage soit disproportionné ou sans rapport avec la finalité du traitement<sup>57</sup>. En l'espèce, contrairement à ce qui prévaut pour Facebook, l'utilisation des fonctionnalités des casques Meta Quest sont segmentés<sup>58</sup>. Les fonctionnalités les plus intrusives (c'est-à-dire le suivi des yeux et des mains et les expressions naturelles du visage) possèdent leur propre politique de confidentialité. De plus, l'utilisateur peut choisir d'utiliser la fonction et de partager les données relatives à son utilisation et il peut également choisir de partager des données supplémentaires. Il n'y a donc pas de pression exercée sur la personne. Si l'utilisateur refuse de partager le suivi des yeux, le service sera certes de moindre qualité mais il ne s'agira pas d'un préjudice puisque seul l'incitant est inutilisable, les autres fonctionnalités du casque restent, elles, disponibles<sup>59</sup>. De plus, au sein même de ces fonctionnalités, leur utilisation est segmentée, ainsi l'utilisateur peut activer la fonction suivi des yeux mais il n'est pas obligé d'activer également la fonction étalonnage du suivi des yeux.

### 1.2. Consentement éclairé

Le consentement est éclairé lorsque la personne est informée de la finalité et de l'étendue du traitement comme le veut le principe de reconnaissabilité (art.6 al.3 nLPD)<sup>60</sup>. Ces informations doivent être fournies d'une manière claire et compréhensible<sup>61</sup>. Elles peuvent être intégrées dans les conditions générales sauf s'il s'agit de clauses insolites (tel que le suivi des yeux) ou si le type de données traitées demande une protection plus étendue<sup>62</sup>. Dans ces cas-là les cases pré-cochées sont interdites et l'attention de la personne doit être attirée sur la signification du

---

<sup>52</sup> SHK DSG–WERMELINGER, DSG 13 N 5.

<sup>53</sup> BSK DSG–RAMPINI, DSG 13 N 3 ; MÉTILLE, Le droit au respect de la vie privée, p. 23.

<sup>54</sup> Bien que le Groupe de travail « article 29 » écrive des lignes directrices quant à l'application du RGPD, les conditions du consentement libre et éclairé sont les mêmes dans le RGPD que dans la nLPD, cf. FF 2017 p. 6647.

<sup>55</sup> G29, p. 6.

<sup>56</sup> G29, p. 12.

<sup>57</sup> MEIER, N 853.

<sup>58</sup> Facebook ne propose pas une telle séparation, le consentement est ainsi donné pour l'ensemble de l'utilisation du réseau social. Si la personne refuse de donner son consentement il ne peut alors pas utiliser le réseau. Le consentement n'est donc pas libre puisque la personne n'a pas un véritable choix, cf. CHARLET, p.85 ; pour aller plus loin sur le concept du « *take it or leave it* » : ZUIDERVEEN BORGESIU, p. 172 ss.

<sup>59</sup> G29, p.12 exemple 9.

<sup>60</sup> CHARLET, p. 88 ; Pour une liste détaillée de ce dont la personne doit être informée : MEIER, N 861.

<sup>61</sup> CHARLET, p.89.

<sup>62</sup> CHARLET, p.89 ; MEIER, N 883 ; D'un autre avis : PRAZ, N 31 qui recommande qu'il y ait toujours un système d'*opt-in*, position qui doit, à notre avis, être suivit.

traitement auquel elle consent<sup>63</sup>. Dans les cas où les informations ne peuvent être intégrées aux conditions générales, la loi ne prévoit pas de quelle manière ces informations doivent être données. Il faut uniquement qu'elles se distinguent des conditions générales, par exemple en superposant les informations<sup>64</sup>. En l'espèce, suivant les fonctionnalités que l'utilisateur décide d'activer, il peut s'agir de données sensibles qui requièrent une information plus claire. C'est bien ce qu'a fait Meta, puisque les fonctionnalités les plus invasives (suivi des yeux, main et expressions naturelles du visage) sont désactivées par défaut. Cependant, selon nous l'attention de l'utilisateur n'est pas suffisamment attiré sur la signification du traitement. Lors de l'activation de la fonctionnalité « suivi des mains », il est juste mentionné que le casque « recueille des informations [...] comme expliqué dans l'avis de confidentialité relatif aux mains ». L'utilisateur est donc envoyé sur une page internet alors que l'information pourrait très bien être donnée directement<sup>65</sup>.

Par ailleurs, le consentement doit être donné avant le traitement, donc les informations nécessaires pour consentir doivent également être données avant<sup>66</sup>. Selon nous, les informations doivent donc être données avant l'achat du casque (*supra* III. 4. *in fine*).

### 1.3. Consentement spécifique

Le consentement doit être donné concernant un traitement déterminé<sup>67</sup>. *In casu*, cette condition n'est pas toujours respectée par Meta. La personne qui consent au partage de données supplémentaires ne sait pas exactement quelles sont ces données supplémentaires (*supra* III. 3.) ni à quelles fins elles seront utilisées. Ainsi, dans la page « Contrôlez les informations que vous partagez avec Meta »<sup>68</sup>, Meta commence par dire que « [I]es données supplémentaires comprennent les données suivantes : [...] ». Avec cette formulation nous nous attendons à trouver une liste exhaustive des données supplémentaires. Cependant, le premier type de données supplémentaires collecté se formule ainsi : « [I]es données sur l'amélioration de l'expérience du produit, telles que : [...] ». Le terme « telle que : » introduit des exemples et non une liste exhaustive, ainsi l'utilisateur ne peut jamais vraiment savoir ce qu'il partage ni comment ses données sont utilisées<sup>69</sup>.

### 1.4. Consentement exprès

Un consentement exprès est requis en cas de traitement de données sensibles ou de profilage à risque élevé effectué par une personne privée (art.6 al.7 nLPD). Le profilage (art.5 lit.f nLPD) consiste en une « [...] évaluation automatisée de données personnelles afin de pouvoir évaluer, d'une manière également automatisée, les caractéristiques de la personne »<sup>70</sup>. Le profilage à risque élevé (art.5 lit.g nLPD) est celui qui permet de faire un profil de la personnalité qui porterait atteinte à la personnalité de la personne concernée<sup>71</sup>.

---

<sup>63</sup> D'un avis différent : ROSENTHAL/STUDER, N 30 qui considèrent que les cases pré-cochées sont toujours possible même en cas de consentement exprès.

<sup>64</sup> G29, p. 17 ; STEINFELD, p. 993.

<sup>65</sup> Du même avis : LOPEZ, I. L'application du RGPD : l'adaptation de la réglementation au métavers, 1) Collecter les données du métavers selon le RGPD, ainsi LOPEZ propose de donner l'information au moment où l'utilisateur crée son compte.

<sup>66</sup> MEIER, N 869 et 893.

<sup>67</sup> CHARLET, p. 86.

<sup>68</sup> <https://bit.ly/3HrDYCB>.

<sup>69</sup> Cela n'est pas nouveau, Facebook présente déjà ce problème depuis longtemps, pour une analyse d'un passage de la politique de confidentialité de Facebook montrant le problème quant à la spécificité : CHARLET, p. 86.

<sup>70</sup> FF 2017 p. 6642.

<sup>71</sup> ROSENTHAL/STUDER, N 27 ; MÉTILLE, la nouvelle loi fédérale sur la protection des données, p. 39.

Un consentement exprès demande un comportement actif, en lien direct avec le traitement des données bénéficiant d'une protection plus étendue<sup>72</sup>. Cocher une case ou opter activement pour certains paramètres sont des exemples de consentement exprès<sup>73</sup>. Selon ROSENTHAL/STUDER, « [...] une personne qui consent à recevoir de la publicité personnalisée ne consent pas en même temps expressément à la mise en œuvre du profilage à risque élevé sous-jacent à cette publicité [...]. Le traitement des données doit donc être *mentionné explicitement* »<sup>74</sup>. En l'espèce, Meta prévoit que « nous [Meta] utilisons votre [l'utilisateur] nom, votre photo de profil et les informations relatives à votre activité sur le Produit MPT (y compris votre utilisation des appareils et des applications Meta Quest) : Pour envoyer du contenu commercial personnalisé[...] »<sup>75</sup>. Il s'agit donc d'un profilage, puisque les données collectées sont utilisées afin d'analyser les préférences personnelles et les intérêts de l'utilisateur pour faire du ciblage publicitaire. Ce profilage doit être considéré à risque élevé puisqu'il permet de créer un profil de personnalité et d'apprécier « les caractéristiques essentielles » de l'utilisateur, comme ses habitudes de consommation<sup>76</sup>. Ce qui est le cas vu que Meta recueille des données concernant les achats effectués par l'utilisateur et les applications qu'il utilise<sup>77</sup>. Le consentement doit donc être exprès, ce qui n'est pas le cas en l'espèce puisque Meta n'est jamais clair quant au traitement et à l'utilisation des données. La politique de confidentialité ne dit jamais clairement « lorsque nous collectons telle donnée, elle sera utilisée à cette fin ». Il y est plutôt employé des termes généraux comme « telle que » ou « par exemple ». Le consentement donné par l'utilisateur ne peut donc être considéré comme exprès faute d'informations nécessaires. En définitive, il résulte de notre analyse qu'il est impossible de justifier le traitement de données personnelles par le consentement, ordinaire ou exprès.

## 2. Intérêt privé prépondérant

L'intérêt privé prépondérant est le motif justificatif le plus invoqué par Meta<sup>78</sup>. Selon MEIER, pour lever l'illicéité du traitement, il faut d'abord établir l'intérêt du responsable du traitement à causer l'atteinte, il faut ensuite confirmer qu'il s'agit d'un intérêt digne de protection, puis il convient de déterminer l'intérêt de la personne concernée à ne pas subir l'atteinte. Enfin, il faut procéder à une pesée d'intérêts entre ceux du responsable du traitement et ceux de la personne concernée<sup>79</sup>. L'intérêt invoqué par le responsable de traitement doit être légitime ou posséder une certaine valeur, ce qui n'est pas le cas lorsque l'intérêt n'est pas directement lié au traitement<sup>80</sup>. L'importance donnée à l'intérêt de la personne concernée à ne pas subir l'atteinte dépend des circonstances. Il faut notamment prendre en considération le type de données traitées (s'il s'agit de données sensibles, cela joue plus en faveur de la personne concernée que s'il s'agit de données ordinaires) et les atteintes que peut créer le traitement<sup>81</sup>. Enfin, gardons à l'esprit que la justification d'une atteinte aux principes énoncés à l'art.6 nLPD ne peut être admise à la légère<sup>82</sup>. Ainsi, même si le responsable de traitement possède un intérêt légitime, celui-ci ne doit

---

<sup>72</sup> ROSENTHAL/STUDER, N 32.

<sup>73</sup> FF 2017 p. 6648.

<sup>74</sup> ROSENTHAL/STUDER, N 32.

<sup>75</sup> META, Politique de confidentialité supplémentaires MPT, II. Comment utilisons-nous vos informations ?, <https://bit.ly/3W6wrNC>.

<sup>76</sup> MEIER, N 514.

<sup>77</sup> META, Politique de confidentialité supplémentaires MPT, I. Quelles informations recueillons-nous ?, Activité du Produit MPT, <https://bit.ly/3W6wrNC>.

<sup>78</sup> META, Bases légales, <https://bit.ly/3ULHwmf>.

<sup>79</sup> MEIER, N 1618.

<sup>80</sup> MEIER, N 1622 s.

<sup>81</sup> *Idem*, N 1624.

<sup>82</sup> ATF 136 II 508, consid. 5.2.4.

pas nécessairement l'emporter sur celui de la personne concernée<sup>83</sup>. L'art. 31 al.2 nLPD contient une liste de situations où l'intérêt du responsable de traitement possède un certains poids dans la pesée d'intérêts<sup>84</sup>. N'entre ici en considération que la lit.a qui porte sur le cas où « le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat et les données traitées concernent le cocontractant ». MEIER précise à ce sujet que cela ne peut pas être invoqué pour traiter les données à des fins publicitaires ou afin de « mieux cibler les prestations »<sup>85</sup>. En l'espèce, la « nécessité contractuelle » est le motif le plus invoqué par Meta, mais le plus souvent à la légère. Ainsi, pour la finalité « fournir les Produits MPT, y compris leurs fonctionnalités », Meta se base sur la « nécessité contractuelle » pour justifier la collecte de données concernant « la fréquence et la durée de vos activités sur les Produits MPT »<sup>86</sup>. Nous ne voyons pas bien le lien entre le fait de fournir les produits MPT ainsi que leurs fonctionnalités et l'analyse de la fréquence et de la durée de l'utilisation desdits produits. Le fait que l'utilisateur utilise le produit signifie que la finalité a été atteinte, il n'y a donc pas lieu d'analyser également la fréquence d'utilisation si ce n'est pour inciter l'utilisateur à rester connecté. Pour donner un autre exemple, Meta se base sur la « nécessité contractuelle » pour justifier la collecte de données afin d'« envoyer du contenu commercial personnalisé [...] », ce qui, comme le dit MEIER, ne peut être considéré comme une nécessité contractuelle.

En définitive, nous sommes d'avis que l'intérêt des utilisateurs à ce que leurs données ne soient pas collectées sans vraie justification prime sur les intérêts de Meta, d'autant plus que les utilisateurs ne sont pas assez informés du but de la collecte ni de leurs données collectées, puisqu'il faut passer par dix pages internet différentes afin de s'en faire une idée.

## V. Conclusion

Il ressort de notre analyse que le cadre juridique posé par la nLPD est suffisant pour protéger les données sensibles des utilisateurs de casques de réalité virtuelle. Les principes prévus à l'art.6 nLPD complétés par les motifs justificatifs de l'art.31 nLPD offrent d'ordinaire une bonne protection. Le problème ne se trouve donc pas au niveau de la loi même, mais bien de son application par Meta. L'entreprise ne respecte aucun des principes de l'art.6 nLPD, et cela ne peut être justifié par un motif justificatif selon l'art.31 nLPD. Meta interprète les principes généraux de la nLPD d'une façon trop restreinte mais fait une interprétation trop large des motifs justificatifs permettant de justifier une atteinte à la personnalité de l'utilisateur. Les politiques de confidentialité sont trop nombreuses (plus de dix) et trop longues. Elles sont écrites dans un langage trop général, ce qui donne à Meta l'opportunité de faire ce que l'entreprise désire avec les données de l'utilisateur. Meta présente ainsi une façade transparente, cependant en prêtant une attention aiguë à ce qui est formulé dans leur politique de confidentialité, on ne peut que remarquer qu'il en va tout autrement.

---

<sup>83</sup> MEIER, N 1627.

<sup>84</sup> *Idem*, N 1632 ; ROSENTHAL/STUDER, N 40 ; SHK DSG–WERMELINGER, DSG 13 N 18.

<sup>85</sup> MEIER, N 1639.

<sup>86</sup> META, Bases légales, <https://bit.ly/3ULHwmf>.

# Bibliographie

## 1. Ouvrages doctrinaux

BAERISWYL Bruno/PÄRLI Kurt (édit.), *Stämpflis Handkommentar zum Datenschutzgesetz*, Berne (Stämpfli) 2015 (cité : SHK DSG–AUTEUR).

CHARLET François, Réseaux sociaux et protection des données : analyse des pratiques de Facebook en regard des exigences des droits européen et suisse de la protection des données, *in* *l'ère numérique et la protection de la sphère privée*, sous la direction des Prof. Astrid Epiney, Prof. Samantha Besson, Prof. Marc Amstutz, Zurich, Bâle, Genève (Schulthess) 2018, p. 77 ss.

DE TERWANGNE Cécile, La nouvelle loi suisse de protection des données dans le contexte international, *in* *La révision de la Loi fédérale sur la protection des données*, sous la direction des Prof. Astrid Epiney, Prof. Samantha Besson, Prof. Marc Amstutz, Zurich, Bâle, Genève (Schulthess) 2022, p. 47 ss.

MAURER-LAMBROU Urs/BLECHTA Gabor-Paul (édit.), *Basler Kommentar, Datenschutzgesetz (DSG) / Öffentlichkeitsgesetz (BGÖ)*, Bâle (Helbing) 2014 (cité : BSK DSG – AUTEUR).

MEIER Philippe, *Protection des données : fondements, principes généraux et droit privé*, Berne (Stämpfli) 2011.

MÉTILLE Sylvain, La (nouvelle) Loi fédérale sur la protection des données du 25 septembre 2020 : des principes, des droits et des obligations, *in* *La révision de la Loi fédérale sur la protection des données*, sous la direction des Prof. Astrid Epiney, Prof. Samantha Besson, Prof. Marc Amstutz, Zurich, Bâle, Genève (Schulthess) 2022, p. 1 ss.

MÉTILLE Sylvain, *Le droit au respect de la vie privée : les défis digitaux, une perspective de droit comparé : Suisse, Bruxelles : Parlement européen* 2018.

ZUIDERVEEN BORGESIOUS Frederik J., *Improving privacy protection in the area of behavioural targeting*, Vol. 33, Pays-Bas (Wolters Kluwer) 2015.

## **2. Documents officiels**

Groupe de travail « article 29 » sur la protection des données (G29), Lignes directrices sur le consentement au sens du règlement 2016/679, 10 avril 2018.

Message du Conseil fédéral concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, 15 septembre 2017, FF 2017 p. 6565 ss.

Préposé fédéral à la protection des données et à la transparence (PFPDT), Guide du traitement des données personnelles dans le secteur privé, 01 septembre 2009 (cité : PFPDT, traitement des données personnelles dans le secteur privé).

## **3. Législation**

Nouvelle loi fédérale du 25 septembre 2020 sur la protection des données (Loi sur la protection des données, nLPD)<sup>87</sup>.

Règlement n°2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO n° L 119 du 4 mai 2016, p. 1 (cité : RGPD).

## **4. Jurisprudences**

ATF 138 II 346.

ATAF 2009/44.

ATF 136 II 508.

---

<sup>87</sup> RS 235.1.

## 5. Sources internet

### i. Articles numériques

Dernière consultation le 06.11.2022

LOPEZ Eléna, Métaverse et données personnelles : gare au futur d'aujourd'hui, <https://dpo-consulting.fr/metavers-et-donnees-personnelles-gare-au-futur-daujourd'hui/>, in DPO Consulting, <https://dpo-consulting.fr/>, 08.06.2022.

### ii. Livres numériques

Dernière consultation le 13.12.2022

PRAZ Emilie M., La protection des données et les réseaux sociaux, [https://jusletter.weblaw.ch/fr/juslissues/2015/785/la-protection-des-do\\_fdb2345c0b.html](https://jusletter.weblaw.ch/fr/juslissues/2015/785/la-protection-des-do_fdb2345c0b.html) in Jusletter, <https://jusletter.weblaw.ch>, 12 janvier 2015.

Dernière consultation le 13.12.2022

ROSENTHAL David/STUDER Samira/LOMBARD Alexandre (pour la traduction), La nouvelle loi sur la protection des données, <https://jusletter.weblaw.ch/fr/juslissues/2020/1045.html> in Jusletter, <https://jusletter.weblaw.ch>, 16.11.2020.

Dernière consultation le 13.12.2022

STEINFELD Nili, « I agree to the terms and conditions » : (How) do users read privacy policies online ? An eye-tracking experiment, <https://www.sciencedirect.com/science/article/pii/S0747563215301692?via%3Dihub> in Computers in Human Behavior, <https://www.sciencedirect.com/journal/computers-in-human-behavior>, 2016.

### iii. Politiques de confidentialité

Dernière consultation le 13.12.2022

META, Avis de confidentialité relatif au suivi des mains, <https://www.meta.com/fr-fr/help/quest/articles/accounts/privacy-information-and-settings/hand-tracking-privacy-notice/>, in Meta, <https://www.meta.com/ch/fr/>, 25.10.2022 (cité : Suivi des mains).

Dernière consultation le 13.12.2022

META, Avis de confidentialité relatif au suivi des yeux, <https://www.meta.com/fr-fr/help/quest/articles/accounts/privacy-information-and-settings/eye-tracking-privacy-notice/>, in Meta, <https://www.meta.com/ch/fr/>, 01.12.2022 (cité : Suivi des yeux).

Dernière consultation le 13.12.2022

META, Contrôlez les informations que vous partagez avec Meta, <https://www.meta.com/fr-fr/help/quest/articles/accounts/privacy-information-and-settings/privacy-controls-meta-quest-pro/>, in Meta, <https://www.meta.com/ch/fr/>, 01.12.2022 (cité : Contrôlez les informations).

Dernière consultation le 13.12.2022

META, Politique de confidentialité supplémentaire de Meta Platforms Technologies, <https://www.meta.com/ch/fr/legal/quest/updated-privacy-policy/>, in Meta, <https://www.meta.com/ch/fr/>, 25.10.2022 (cité : Politique de confidentialité supplémentaire MPT).

Dernière consultation le 13.12.2022

META, Politique de confidentialité supplémentaire de Meta Platforms Technologies Bases légales, <https://www.meta.com/ch/fr/legal/quest/legal-bases/>, in Meta, <https://www.meta.com/ch/fr/>, date inconnue (cité : Bases légales).

## Table des équivalences

<https://bit.ly/3W6wrNC> = [https://www.meta.com/ch/fr/legal/quest/privacy-policy/?utm\\_source=www.meta.com&utm\\_medium=dollyredirect](https://www.meta.com/ch/fr/legal/quest/privacy-policy/?utm_source=www.meta.com&utm_medium=dollyredirect)

<https://bit.ly/3VO7HtU> = <https://www.meta.com/fr-fr/help/quest/articles/accounts/privacy-information-and-settings/hand-tracking-privacy-notice/>

<https://bit.ly/3ULHwmf> = <https://www.meta.com/ch/fr/legal/quest/legal-bases/>

<https://bit.ly/3VMb58I> = <https://www.meta.com/fr-fr/help/quest/articles/accounts/privacy-information-and-settings/eye-tracking-privacy-notice/>

<https://bit.ly/3HrDYCB> = <https://www.meta.com/fr-fr/help/quest/articles/accounts/privacy-information-and-settings/privacy-controls-meta-quest-pro/>