Global Guideline

Online Research

ESOMAR
WORLD RESEARCH

GLOBAL RESEARCH
BUSINESS NETWORK
APRC • EFAMRO • ARIA

ESOMAR, association mondiale pour les études de marché, études sociales et d'opinion, est l'organisation essentielle pour encourager, faire avancer et élever le secteur des études de marché. www.esomar.org

GRBN (Global Research Business Network), réseau international pour la recherche professionnelle, regroupe 38 associations de recherche et plus de 3 500 sociétés spécialisées dans la recherche issues des cinq continents. www.grbn.org

Official Translation Partner:
Language Connect

TABLE DES MATIÈRES

1 INTRODUCTION ET PORTÉE

En 2011, ESOMAR a publié une Directive pour la réalisation des enquêtes en ligne, à l'issue d'un travail en collaboration avec CASRO. En 2015, la Directive ESOMAR/GRBN sur la qualité des échantillons en ligne fut publiée. Les chercheurs sont encouragés à consulter ce dernier document ainsi que la présente directive durant la conception et la réalisation des enquêtes en ligne.

Bien que des solutions à de nombreux problèmes techniques et méthodologiques liés à la recherche en ligne aient été trouvées au cours de la dernière décennie, les développements technologiques continus ainsi que la multiplication des types et de la variété des données numériques pouvant être collectées en ligne impliquent des révisions et mises à jour systématiques des recommandations professionnelles et éthiques.

La présente Directive ESOMAR/GRBN pour la recherche en ligne a une portée internationale et explique comment appliquer certains des principes fondamentaux relatifs aux études de marché, études sociales et d'opinion dans le contexte des cadres juridiques et réglementaires actuellement en vigueur dans le monde entier. Ainsi, ce document est davantage une déclaration de principes qu'un catalogue des réglementations existantes. Son objectif est de soutenir les chercheurs, en particulier ceux travaillant pour de petites et moyennes organisations de recherche, pour ce qui est des questions juridiques, éthiques et pratiques dans le cadre de l'utilisation des nouvelles technologies lors de la réalisation d'enquêtes en ligne.

Cette directive n'a pas pour but de se substituer à la lecture attentive et à la compréhension du Code international ICC/ESOMAR des études de marché et d'opinion, qui a été adopté par plus de 60 associations locales dans le monde entier, ni aux codes individuels des 38 associations qui constituent le GRBN. Elle a au contraire été conçue comme une interprétation des principes fondateurs de ces codes, dans le contexte de la recherche en ligne.

Il est également essentiel que les chercheurs vérifient et se conforment aux obligations d'auto-réglementation nationales et locales concernant la protection des données et les études de marché, dans chaque pays où ils prévoient de collecter et de traiter des données, étant donné que des différences concernant la façon dont les principes de base sont appliqués dans un pays spécifique peuvent exister. Les recommandations fournies dans le présent document constituent un standard minimum et peuvent avoir besoin d'être complétées par des mesures supplémentaires dans le cadre d'un projet de recherche précis. Les chercheurs pourraient juger nécessaire de consulter un conseiller juridique local dans la juridiction où la recherche est menée afin de s'assurer qu'ils se conforment pleinement à leurs obligations.

Les chercheurs doivent être sensibles aux préoccupations des consommateurs et garder à l'esprit que la réussite d'une étude de marché repose sur la confiance du public. Les chercheurs doivent éviter les activités et les pratiques technologiques qui risquent de miner la confiance du public dans les études de marché. Cela implique l'application de principes et de pratiques méthodologiques fiables lors de la conception de l'enquête, en particulier pour garantir que la conception du questionnaire, la durée et la charge pour le participant soient appropriées. Ils doivent également assidument maintenir une distinction entre leurs activités de recherche et leurs activités commerciales comme le marketing direct ou la publicité ciblée. Lorsque les chercheurs sont impliqués dans des activités utilisant des techniques de recherche qui n'ont pas pour seule vocation la recherche, ils ne doivent pas décrire ces activités comme un projet d'étude de marché, d'étude sociale ou d'opinion.

Tout au long de ce document, le mot « doit/doivent » est utilisé pour signifier des exigences obligatoires. Nous utilisons le mot « doit/doivent » pour décrire un principe ou une pratique que les chercheurs sont tenus de respecter. Le mot « devrait/devraient » est utilisé pour décrire une application. Cet usage vise à signifier le fait que les chercheurs ont la possibilité

de décider d'appliquer un principe ou une pratique de diverses manières en fonction de la conception de leur projet de recherche.

2 DÉFINITIONS

Technologies à agents actifs fait référence à des technologies qui enregistrent le comportement des participants aux projets de recherche en arrière-plan et qui fonctionnent habituellement parallèlement à d'autres activités. Elles comprennent :

- Les logiciels de suivi qui enregistrent le comportement en ligne véritable des participants aux projets de recherche, comme les pages web consultées, les transactions en ligne réalisées, les formulaires en ligne complétés, les taux de clics ou impressions publicitaires, les achats en ligne et les informations de géolocalisation pour les appareils informatiques dotés d'une connexion Internet. Ces logiciels sont également capables d'enregistrer des informations tirées des e-mails du participant et des autres documents stockés sur un appareil tel qu'un disque dur. Certaines de ces technologies ont été qualifiées de « logiciels espions », en particulier lorsque le téléchargement, l'installation ou la collecte de données se produit sans que les participants n'en soient pleinement conscients et ne donnent leur accord.

- Les logiciels téléchargés sur l'appareil informatique d'un utilisateur (ordinateur, tablette, smartphone, etc.) qui sont uniquement utilisés afin d'avertir les potentiels participants aux projets de recherche des opportunités d'enquête, de télécharger le contenu de l'enquête ou de poser des questions d'enquête. Ils ne suivent pas les participants aux projets de recherche lorsqu'ils naviguent sur Internet et toutes les données collectées sont fournies directement et de manière proactive par l'utilisateur.

Recherche active fait référence à la collecte de données issue d'une interaction directe avec le participant au projet de recherche (par ex. une enquête, un groupe de discussion ou une autre méthodologie d'enquête, en personne ou via d'autres moyens de communication, par ex. par téléphone, par courrier ou en ligne, y compris par e-mail, SMS ou tout autre moyen technologique).

Recherche Business-to-business (B2B) fait référence à la collecte de données auprès de ou à propos d'entités juridiques telles que des entreprises, des écoles, des organisations à but non lucratif, etc.

Recherche Business-to-consumer (B2C) fait référence à la collecte de données auprès de ou à propos d'individus ou de foyers.

Cloud computing fait référence au déploiement de groupes de serveurs et de réseaux informatiques à distance qui permettent un stockage centralisé de données et un accès en ligne à des services et ressources informatiques. Le cloud computing comprend trois modèles généraux de déploiement : public, privé ou hybride.

Activité commerciale fait référence à une activité dont l'objectif n'est pas la recherche, comme le marketing direct et la publicité ciblée.

Consentement fait référence à l'accord informé et donné librement par une personne quant à la collecte et au traitement de ses données personnelles.

Cookies fait référence à des fichiers textes contenant de petites quantités d'information, qui sont téléchargés sur l'appareil de l'utilisateur lorsqu'il visite un site Internet. Les cookies sont lus ou renvoyés au site web d'origine à chaque visite ultérieure, ou vers un autre site web reconnaissant ce cookie.

Les cookies sont utiles car ils permettent à un site web de reconnaître l'appareil d'un utilisateur, et ainsi de personnaliser l'expérience de l'utilisateur. Ils sont notamment capables d'enregistrer les préférences de l'utilisateur et généralement de rendre la navigation sur le site web plus efficace. Les chercheurs sont susceptibles d'utiliser des cookies à diverses

fins, notamment pour assurer une expérience d'enquête, un contrôle de la qualité et une validation améliorés, pour permettre ou faciliter la participation à une enquête, pour suivre le nombre d'enquêtes terminées ou les autres actions réalisées, et pour détecter et/ou prévenir la fraude. Les cookies peuvent être rejetés ou supprimés grâce à une fonction dans les paramètres de configuration des navigateurs.

Contrôleur de données fait référence à une personne ou une organisation responsable de déterminer la façon dont les données personnelles sont traitées. Par exemple, un chercheur serait le contrôleur de données de ses clients ; un fournisseur de panel de recherche serait le contrôleur des données collectées auprès de ses membres de panel en ligne ; et une entreprise de recherche serait le contrôleur des données collectées auprès des participants dans le cadre d'une enquête omnibus.

Gestionnaire de données fait référence à une partie qui obtient, enregistre, détient ou effectue des opérations (y compris des analyses) sur des données personnelles au nom de et sous la direction du contrôleur de données. Comme indiqué ci-dessus, une entreprise de recherche serait à la fois le contrôleur de données et le gestionnaire de données dans le cadre d'une enquête omnibus**.**

Identifiant d'appareil fait référence à un numéro précis associé à un smartphone ou tout appareil portable similaire. Un tel appareil dispose habituellement de plusieurs identifiants d'appareil, chacun utilisé à une fin différente. Certains identifiants d'appareils sont utilisés pour permettre d'activer des services tels que le Wi-Fi ou le Bluetooth, ou pour distinguer divers appareils fonctionnant sur le réseau d'un opérateur mobile. Les autres identifiants d'appareil, tels que l'UDID d'Apple ou l'Android ID d'Android, sont utilisés par les applications, les développeurs et d'autres entreprises pour identifier, suivre et analyser les appareils et leurs utilisateurs sur divers services mobiles.

Empreinte numérique (également appelée empreinte d'appareil, empreinte de machine ou empreinte de navigateur) fait référence à des informations recueillies à propos d'un appareil informatique (ordinateur, tablette, smartphone, etc.) à des fins d'identification. Les empreintes numériques peuvent être utilisées afin d'identifier entièrement ou en partie des participants aux projets de recherche ou des appareils précis lorsque les cookies sont désactivés. Elles se basent généralement sur des informations de configuration de navigateur web, ainsi que d'autres paramètres d'appareil informatique qui peuvent être obtenus. Ces informations sont regroupées dans une même chaîne qui constitue l'empreinte numérique. Les empreintes numériques sont également utilisées à d'autres fins que la recherche et se sont avérées utiles pour détecter le vol d'identité en ligne et pour la prévention des utilisations frauduleuses des cartes bancaires.

Dans certaines juridictions, les empreintes numériques peuvent être considérées comme des données personnelles et doivent être traitées comme telles, y compris en ce qui concerne le besoin de consentement.

Il est important de noter qu'étant donné que certains éléments composant l'empreinte numérique peuvent changer avec le temps, l'empreinte numérique associée à un appareil peut également varier.

Dans les études de marché, le terme identifiant d'appareil est parfois utilisé pour désigner l'empreinte numérique. Toutefois, identifiant d'appareil a une autre signification (cf. identifiant d'appareil).

Tirage au sort ou concours gratuits fait référence à un concours ou un tirage dans le cadre desquels des prix sont remis au hasard, sans que le participant n'ait à payer ou prendre une mesure autre que celle de s’inscrire pour avoir une chance de gagner. Bien que ces derniers soient parfois désignés sous le terme de loterie, dans de nombreuses juridictions, une loterie correspond à un terme juridique très précis et est souvent interdite pour les entités privées telles que les instituts de recherche.

Géolocalisation fait référence à la détermination de l'emplacement géographique réel d'un objet, tel qu'un appareil informatique (ordinateur, tablette, smartphone, etc.). La géolocalisation peut faire référence à la pratique d'évaluer l'emplacement, ou à l'emplacement évalué lui-même.

Rétribution fait référence à un avantage offert à un participant pour l'encourager à participer à un projet de recherche.

Lois sur la protection des données fait référence aux lois et réglementations nationales et locales dont l'application a pour effet de protéger les données personnelles conformément aux principes présentés dans le présent document**.**

Objets locaux partagés, communément appelés cookies Flash (en raison de leurs similarités avec les cookies HTTP), sont des données que les sites web utilisant Adobe Flash peuvent stocker sur l'appareil ou l'ordinateur d'un utilisateur.

Études de marché, y compris les études sociales et d'opinion, fait référence à la collecte et à l'interprétation systématiques d'informations concernant des individus ou organisations utilisant des méthodes et techniques statistiques et analytiques tirées des sciences sociales et comportementales pour acquérir des aperçus et appuyer les prises de décision.

Recherche en ligne fait référence à l'utilisation de réseaux informatiques, en particulier l'Internet, pour aider à n'importe quel stade du processus d'étude de marché, y compris le développement de la problématique, la conception du projet de recherche, la collecte de données, ou l'analyse.

Données périphériques fait référence aux données relatives au processus ayant permis de collecter les données de l'enquête. Cela comprend la date et l'heure auxquelles l'enquête a été complétée, le temps qu'a duré l'enquête, et la navigation du participant dans l'enquête.

Recherche passive fait référence à la collecte de données en observant, mesurant ou enregistrant les actions ou le comportement d'un utilisateur.

Données personnelles fait référence aux informations en lien avec une personne physique identifiée ou identifiable. Une personne identifiable est une personne qui peut être identifiée directement ou indirectement, en particulier en se référant à un numéro d'identification ou aux caractéristiques physiques, physiologiques, mentales, économiques, culturelles ou sociales de la personne. Dans certains types de projets de recherche, de telles archives de données pourraient comprendre des situations ou les individus sont identifiables en raison de photos, vidéos et enregistrements audio, ou d'autres données personnelles collectées durant le projet de recherche.

PII (Personally identifiable information) est l'acronyme anglais désignant les informations d'identification personnelle. Voir données personnelles.

Cloud privé désigne un arrangement de cloud computing où du matériel dédié dans un centre de données particulier est assigné à la société du chercheur.

Cloud public désigne un arrangement de cloud computing où un fournisseur de services met à disposition du grand public des ressources sur Internet, telles que des applications et des solutions de stockage.

Participant au projet de recherche désigne toute personne dont les données personnelles sont collectées à des fins de recherche, que ce soit par des moyens actifs ou passifs.

Chercheur désigne un individu ou une organisation qui réalise, ou fait office de consultant, dans le cadre d'un projet de recherche, y compris ceux qui travaillent pour les entreprises clientes et les sous-traitants auxquels il est fait appel.

Données sensibles fait référence aux informations concernant l'origine raciale ou ethnique, la santé ou l'orientation sexuelle, les antécédents judiciaires, l'opinion politique, les croyances religieuses ou philosophiques ou l'appartenance éventuelle à un syndicat d'un

individu précis. D'autres informations pourraient être considérées comme sensibles dans d'autres juridictions. Aux États-Unis par exemple, les informations en lien avec la santé personnelle, les revenus ou les autres informations financières, les identifiants bancaires et les documents émis par le gouvernement ou révélant les coordonnées bancaires sont également considérées comme sensibles.

Recherche sur réseaux sociaux fait référence à une sorte de projet de recherche dans le cadre duquel des données tirées des réseaux sociaux sont utilisées soit seules, soit en conjonction avec des données issues d'autres sources.

Logiciel espion désigne un logiciel se saisissant du contrôle d'un ordinateur ou recueillant des informations à propos d'une personne ou d'une organisation, sans que l'utilisateur n'en soit informé, et susceptible de renvoyer ces informations à une autre entité sans le consentement de l'utilisateur.

Sous-traitance fait référence à l'action de transférer la responsabilité d'exécuter une partie du projet de recherche à une organisation ou un individu tiers. Cela comprend l'externalisation et la délocalisation (offshoring).

Pixels espions fait référence à des objets discrets (généralement invisibles pour l'utilisateur) hébergés sur une page web ou un e-mail. Les pixels espions permettent à l'opérateur d'une page web ou à l'expéditeur d'un e-mail de déterminer si un utilisateur a visualisé la page ou l'e-mail. On les utilise souvent pour le suivi d'e-mails et le balisage de pages à des fins d'analyse web. On les appelle également balises web, mouchards, pixels invisibles ou encore web bug.

Transferts en ce qui concerne les données, fait référence à toute divulgation, communication, copie ou déplacement de données d'une partie vers une autre, quel que soit le support, y compris les déplacements au sein d'un réseau, les transferts physiques, les transferts d'un support ou appareil à un autre, ou au travers d'un accès à distance aux données.

Transferts transfrontaliers de données personnelles fait référence au déplacement de données personnelles au-delà des frontières nationales, par quelque moyen que ce soit, y compris l'accès à des données depuis un autre pays que celui où elles ont été collectées. Cela peut impliquer l'utilisation de technologies sur le cloud pour la collecte et le stockage de données**.**

3 PARTICIPANTS : RELATIONS ET RESPONSABILITÉS

3.1 Distinguer les études de marché, études sociales et d'opinion des autres activités impliquant la collecte de données

Les chercheurs doivent s'assurer que les objectifs de la recherche sont clairement distingués des autres activités en ligne ne relevant pas de la recherche. En outre, ils ne doivent pas autoriser l'utilisation des données personnelles qu'ils recueillent pour toute autre fin que les études de marché. Afin de clairement communiquer cette distinction aux participants au projet de recherche, le chercheur doit présenter les services de recherche et l'organisation ou l'entreprise qui les entreprend de telle manière qu'ils soient clairement différenciés des activités ne relevant pas de la recherche.

Cette exigence n'empêche pas les chercheurs d'être impliqués dans des activités ne relevant pas de la recherche, tant que l'objectif de la collecte des données personnelles n'est pas déformé et que les données personnelles ne sont pas utilisées à une autre fin, sauf si un consentement éclairé spécifique est obtenu de la part du participant. Elle ne limite pas non plus le droit d'une organisation de promouvoir le fait qu'elle mène à la fois des études de marché et d'autres activités, tant qu'elles sont clairement différenciées et qu'elles sont réalisées séparément et conformément aux lois, réglementations et règles de conduite en vigueur.

3.2 Notification, honnêteté, consentement et la nature volontaire de la recherche

Les chercheurs doivent obtenir le consentement éclairé des participants au projet de recherche avant de collecter et de traiter toute forme de données personnelles, et doivent être parfaitement transparents quant aux informations qu'ils prévoient de collecter, la fin à laquelle elles seront collectées, la façon dont elles seront protégées, avec qui elles pourront être partagées, et sous quelle forme. Ces informations doivent être claires, concises et voyantes. Cela implique notamment l'utilisation de bonnes pratiques dans le cadre des politiques de confidentialité, le placement évident de liens vers les politiques de confidentialité dans les questionnaires et sur les sites de panels, et une bonne communication tout au long de la collecte de données et des processus d'utilisation des données. Les participants ne doivent jamais être induits en erreur, dupés ou contraints et il ne doit jamais leur être menti. La participation à un projet de recherche se fait toujours sur une base volontaire et les participants doivent être autorisés à se retirer ainsi qu'à exiger la suppression de leurs données personnelles, dans la mesure où elles ne sont pas enregistrées sous forme de pseudonyme, à tout moment.

La présente Directive reconnaît également que l'obtention du consentement peut ne pas être possible dans certaines situations. Cf. point 3.2.1 pour plus de détails.

Si à un moment quelconque durant le projet de recherche des changements matériels sont apportés au plan de recherche (par exemple une collecte passive de données supplémentaires comme l'emplacement ou des données identifiables partagées avec les clients utilisateurs de la recherche), les participants doivent en être informés afin que leur décision de poursuivre l'enquête ou non puisse faire l'objet d'un choix éclairé. Dans le cas d'un access panel ou d'une communauté de recherche, ou lorsque la recherche implique plusieurs vagues de collecte de données ou s'étend sur plusieurs mois, les chercheurs doivent régulièrement réobtenir le consentement en rappelant aux participants les données collectées, les raisons de la collecte et l'usage prévu des données. Le consentement doit être réobtenu notamment lorsqu'un changement matériel est apporté aux pratiques de collecte et d'utilisation de données, lors d'un changement concernant l'organisation ou la propriété du projet de recherche, ou lors d'un changement concernant les lois et réglementations en vigueur.

Enfin, les chercheurs doivent se soumettre à l'ensemble des lois, réglementations et règles de conduite professionnelles en vigueur.

3.2.1 Données passives

Les nouvelles technologies rendent désormais possible le fait de collecter un large éventail de données personnelles, sans interaction directe avec les individus dont les données sont recueillies.

Cela inclut par exemple les données de navigation web, les analyses de cartes de fidélité et de magasin, les données de géolocalisation fournies par des appareils connectés et certains types de données issues des réseaux sociaux. Avec l'évolution constante des technologies mobiles, un grand nombre de ces sources de données est également accessible depuis des appareils mobiles.

Dans les situations où les chercheurs recueillent des données de navigation sur plusieurs sites auprès de membres de panels ou par l'intermédiaire d'applications mobiles, une description détaillée des données spécifiques collectées et de la/des méthode(s) utilisée(s) pour les collecter doit être fournie au participant et son consentement explicite doit être obtenu avant la collecte desdites données. Cela est notamment le cas pour les applications mobiles qui nécessitent une géolocalisation, une écoute passive, et/ou une surveillance du système d'exploitation des appareils mobiles.

Lorsque les données personnelles sont collectées depuis des espaces publics tels que des sites web ou des réseaux sociaux, un consentement doit être obtenu directement ou explicitement prévu dans les conditions d'utilisation de la plateforme. Cela ne s'applique pas aux publications sur les réseaux sociaux qui comprennent le nom de l'auteur, ce qui implique une baisse attendue de la confidentialité.

Certaines associations, y compris CASRO et ESOMAR, disposent de directives spécifiques relatives aux réseaux sociaux qui doivent être consultées pour de plus amples informations. Une directive combinée ESOMAR/GRBN sur les réseaux sociaux est actuellement en cours de développement et sa publication est prévue pour début 2016.

Lorsque les chercheurs font appel à des tierces parties pour la collecte de données, il est de la responsabilité du chercheur de s'assurer que les données ont été obtenues en toute légalité.

Étant donné que des différences concernant la façon dont les réglementations sont appliquées dans un pays spécifique peuvent exister,[1] il est également essentiel que les chercheurs vérifient et se conforment aux obligations d'auto-réglementation nationales et internationales concernant la protection des données et les études de marché, dans chaque pays où ils prévoient de collecter et de traiter des données.

Si les chercheurs transfèrent des commentaires à une tierce partie sans consentement, ils doivent veiller à ne rapporter que des données rendues anonymes en utilisant des techniques permettant par exemple de masquer les commentaires.

Lorsqu'elles mènent leurs projets de recherche, les sociétés de recherche doivent fournir une politique de confidentialité claire et accessible concernant leurs pratiques en matière de collecte de données et de confidentialité, expliquant notamment comment contacter la société de recherche.

En outre, le chercheur est tenu de protéger la confidentialité et la sécurité de toute donnée personnelle de quelque manière qu'elle ait été obtenue. Cela implique pour la société de recherche de rendre les données anonymes avant de les partager avec des tiers, et de conclure un contrat avec le destinataire des données dans le cadre duquel ce dernier accepte de ne pas tenter de ré-identifier des individus, ni d'utiliser ces données à fins ne relevant pas de la recherche.

3.2.2 Données sensibles

Bien que la méthodologie en ligne constitue un mode de collecte de données moins intrusif que les autres, et qu'elle permette aux chercheurs d'aborder des sujets sensibles plus facilement qu'au travers d'entretiens en face à face ou par téléphone (en la présence d'un enquêteur), les chercheurs doivent malgré tout être prudents lorsqu'ils soumettent aux participants des sujets de nature sensible, soit en raison de réglementations juridiques, soit pour ne pas causer de préjudice ou mettre en difficulté le participant.

Les chercheurs doivent veiller à expliquer l'objectif des questions sensibles de l'enquête, obtenir le consentement explicite du participant, mentionner que le traitement des données se déroule de manière anonyme et confidentielle, prévoir une option « préfère ne pas répondre » à chaque question, ou une autre option permettant au participant de ne pas répondre à la question sensible s'il ne souhaite pas y répondre, et s'assurer que les questions sont nécessaires, pertinentes et claires. Si ces protections ne peuvent pas être fournies à cause de la conception de l'enquête, le participant doit en être informé et doit donner son consentement explicite.

[1] Le consentement est obligatoire dans de nombreuses juridictions afin de collecter, traiter et partager les données personnelles. Certaines juridictions sont susceptibles d'autoriser des exceptions pour la recherche, lorsqu'il peut être démontré que l'obtention du consentement ne peut être garantie, et si l'analyse fournie au client se présente sous forme de données rendues anonymes.

Dans certains pays, il peut être nécessaire d'obtenir l'autorisation de recueillir les données personnelles à caractère sensible auprès des autorités nationales pertinentes.

3.3 Assurer l'absence de préjudices

Les chercheurs doivent prendre toutes les précautions raisonnables pour s'assurer qu'aucun préjudice ou tort ne soit causé aux participants au projet de recherche en ligne dans le cadre de leur participation. Cela comprend n'importe quel type de préjudice, par exemple financier, physique ou émotionnel. Ainsi, ils devraient examiner avec soin les exigences spécifiques liées au projet de recherche, consulter les exigences/restrictions et réglementations juridiques locales, et étudier les implications pratiques que peut avoir l'enquête sur les participants. Dans tous les cas, les chercheurs doivent respecter les principes de traitement équitable. Ces derniers comprennent :

- éviter d'effectuer des déclarations trompeuses susceptibles de causer un préjudice ou d'occasionner une gêne pour le participant (par ex. informations inexactes sur le contenu du projet de recherche, sur la durée probable de l'entretien, ou sur la possibilité d'être réinterviewé ultérieurement par l'intermédiaire de techniques en ligne ou autres) ;

- éviter la collecte et l'analyse trompeuses ou non sollicités des données (par ex. avec des systèmes automatisés non déclarés qui collectent des données personnelles dans des environnements en ligne/sur des appareils mobiles) là où les utilisateurs s'attendent à un certain niveau de confidentialité et à ce qu'on leur demande leur consentement vis-à-vis d'actions spécifiques ; et

- répondre à toute requête que les participants sont susceptibles d'adresser à l'agence/au chercheur responsable de l'étude de marché.

Le chercheur doit s'assurer que les données personnelles ne puissent pas être suivies, ni qu'il soit possible d'interférer avec l'identité d'un individu suite à une analyse croisée (divulgation déductive), à cause de petits échantillons ou de toute autre manière au travers des résultats de l'enquête. Cela comprend par exemple la fusion d'informations auxiliaires telles que des données concernant la zone géographique ou la capacité d'identifier un participant spécifique à un projet de recherche.

3.4 Protection des données et confidentialité

Les chercheurs doivent respecter les principes universels de protection des données concernant les données personnelles. Ces principes édictent que toute information personnelle collectée et détenue doit être :

- collectée à des fins de recherche précises et ne doit pas être utilisée d'une manière incompatible avec ces fins ;

- adéquate, pertinente et non excessive vis-à-vis des objectifs du projet de recherche pour lequel elle a été collectée et/ou traitée ultérieurement ;

- stockée séparément des données de réponses si possible ; et

- conservée pas plus longtemps que le temps nécessaire à la réalisation de l'objectif pour lequel l'information a été collectée ou traitée ultérieurement.

Les chercheurs doivent également se soumettre à l'ensemble des lois et réglementations nationales et locales en vigueur.

3.4.1 Politiques de confidentialité

Toutes les lois et réglementations sur la confidentialité exigent habituellement que les sociétés de recherche publient une politique de confidentialité sur leur site web. Ces

politiques de confidentialité doivent indiquer aux participants aux projets de recherche quelles informations personnelles sont collectées, de quelle manière elles sont utilisées, comment elles seront gérées (stockage et accès) et partagées, et les conditions sous lesquelles elles peuvent être divulguées à des tierces parties. Les politiques de confidentialité doivent également décrire comment obtenir de plus amples informations ou déposer une plainte. Elles doivent aussi être mises à disposition (généralement sous forme d'un lien) dans tous les projets de recherche en ligne ainsi que sur les sites web concernés et dans les courriers électroniques.

Les participants doivent également être informés des lois régissant la collecte des données. Si des données sont collectées dans plusieurs pays, le chercheur doit se soumettre aux lois des pays dans lesquels le projet de recherche est mené. Lorsqu'il est possible de connaître le pays de résidence du participant, les chercheurs doivent suivre les exigences légales de ce pays, en sachant que des variations considérables peuvent exister entre les diverses juridictions.

3.4.2 Sécurité des données

Les chercheurs doivent veiller à appliquer des protocoles de sécurité protégeant contre les risques tels que la perte, l'accès non autorisé, la destruction, l'utilisation, la modification et la divulgation. Ainsi, les chercheurs doivent déployer des mesures de sécurité des données rigoureuses.

Les chercheurs peuvent utiliser plusieurs normes et cadres de travail pour développer les normes et politiques de sécurité des données nécessaires. Pour en savoir plus, les chercheurs peuvent consulter la norme ISO/IEC 27001 – Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences ou la Checklist ESOMAR sur la protection des données.

3.4.3 Notification des violations

Les chercheurs doivent se soumettre à toutes les lois et réglementations en vigueur concernant la notification des violations et les exigences protocolaires. En l'absence de telles lois et réglementations, les chercheurs doivent rapporter les violations de sécurité ou de données à toutes les parties affectées, y compris les clients, les participants au projet de recherche et les sous-traitants, dans les meilleurs délais. La notification doit inclure une description des types de données ayant subi cette violation et toutes les mesures que devront prendre les individus pour se protéger d'un éventuel préjudice pouvant découler de la violation.

3.4.4 Transferts transfrontaliers

Avant que les données personnelles ne soient transférées depuis le pays de collecte vers un autre pays, le chercheur doit s'assurer que le transfert de données est légal, et que toutes les mesures raisonnables sont prises pour garantir la confidentialité et la sécurité de ces données. Cela s'applique si le serveur de collecte de données est situé dans un autre pays. Ce principe s'applique également si une technologie de cloud est utilisée et que les serveurs cloud sont situés dans un autre pays (cf. point 7.7).

3.5 Sollicitation par e-mail et SMS

Les lois locales et nationales concernant le traitement des e-mails et des SMS sont susceptibles de varier. Dans certains pays, l'utilisation de systèmes automatisés pour envoyer des SMS est interdite sauf si un consentement explicite a été obtenu.[2] Les

[2] Encore une fois, les lois et réglementations concernant l'utilisation de systèmes automatisés pour la composition d'un numéro de téléphone et l'envoi de SMS sur les téléphones mobiles varient selon les juridictions. Dans certaines juridictions, il existe des exceptions pour la recherche, tandis que dans d'autres, un consentement est requis. Il convient de souligner qu'aux États-Unis, la loi sur la protection des consommateurs concernant le téléphone (Telephone Consumer Protection Act) exige qu'un consentement soit obtenu pour composer un numéro et envoyer un SMS à un téléphone mobile par l'intermédiaire de systèmes automatisés.

chercheurs ne doivent pas utiliser un subterfuge quelconque pour obtenir les adresses e-mail ou les numéros de téléphone mobile de participants potentiels. Cela comprend l'utilisation de domaines publiques, l'utilisation de technologies ou de techniques sans que l'individu n'en ait conscience, ou la collecte sous prétexte d'une activité autre que la recherche.

Les chercheurs ne doivent pas utiliser des e-mails ou SMS non sollicités pour recruter des participants aux projets de recherche ou pour lancer des collectes de données clandestines. « Non sollicité » signifie ici que les participants n'ont pas donné leur accord ou ne s'attendent pas raisonnablement à recevoir de tels e-mails ou SMS.

Les individus contactés à des fins de recherche par e-mail ou SMS doivent comprendre qu'ils pourraient recevoir un contact par e-mail ou SMS concernant un projet de recherche. On peut partir du principe que l'accord a été donné lorsque TOUTES les conditions suivantes sont réunies ET qu'il n'existe pas de restrictions ou d'interdictions en vertu de lois et/ou réglementations locales :

- Une relation préexistante réelle existe entre les individus contactés et le chercheur, le client fournissant les adresses e-mail ou les numéros de téléphone mobile, ou les fournisseurs d'échantillons fournissant les adresses e-mail ou les numéros de téléphone (l'invitation par e-mail ou SMS faisant clairement mention de ce dernier ou renvoyant à son nom par l'intermédiaire d'un lien).

- Lorsque les personnes invitées par e-mail ou SMS ont spécifiquement consenti au projet de recherche en ligne ou sur mobile avec le chercheur ou le fournisseur d'échantillons, ou dans le cas d'une liste de clients fournie par le client où ces derniers n'ont pas refusé les communications par e-mail ou SMS, et peuvent être contactés dans le cadre du projet de recherche.

- Les invitations par e-mail ou SMS envoyées aux participants potentiels au projet de recherche mentionnent clairement ou renvoient vers le nom du fournisseur d'échantillons, du chercheur ou du client, et leur relation avec l'individu, et offrent clairement la possibilité d'être supprimé de la liste de diffusion par e-mail ou SMS.

- Tous les individus ayant précédemment demandé à ne plus être contactés par e-mail ou SMS à l'avenir sont supprimés de manière appropriée et en temps opportun de la liste de l'échantillon par e-mail ou de numéros de téléphone mobile.

- Les participants figurant dans les échantillons par e-mail ou SMS n'ont pas été recrutés par l'intermédiaire d'invitations par e-mail ou SMS non sollicitées.

Les chercheurs doivent également noter que :

- Lorsqu'ils reçoivent des listes d'e-mails ou des listes de numéros de téléphone de leurs clients ou de fournisseurs d'échantillons, les chercheurs doivent vérifier auprès du client ou du fournisseur d'échantillons si les individus listés peuvent raisonnablement s'attendre à être contactés par e-mail ou par SMS.

- Les chercheurs ne doivent pas utiliser d'adresses e-mail de retour factices ou trompeuses ou toute autre information fausse et trompeuse lorsqu'ils recrutent des participants.

- Les chercheurs doivent donner la possibilité aux participants de refuser de participer à n'importe quel projet de recherche. Cela s'applique également si un participant demande à être supprimé de la liste de la source d'échantillon pour les études à l'aveugle (c.-à-d.

lorsque le sponsor de l'étude n'est pas cité ou qu'aucun lien ne mène à lui dans la sollicitation par e-mail ou SMS, mais que son nom peut être révélé au participant durant ou au terme de l'entretien).

- Les chercheurs doivent se soumettre à toute exigence applicable indiquée dans cette section lorsqu'ils utilisent d'autres technologies de messagerie, telles que les applications mobiles, pour envoyer des notifications qui ont des caractéristiques et capacités semblables aux SMS.

Il est recommandé aux chercheurs de conserver des copies ou des archives des e-mails et des autres documents reçus de la part des participants aux projets de recherche acceptant ou restreignant l'accès et l'utilisation de leurs informations personnelles.[3]

3.6 Rétributions

Les règles concernant les concours et les tirages au sort gratuits doivent être lues en parallèle des règles suivantes sur les rétributions.

Lorsque des rétributions sont offertes pour encourager la participation aux projets de recherche en ligne, les chercheurs doivent s'assurer que les participants sont clairement informés de :

- qui remettra les rétributions ;
- quelles seront les rétributions ;
- quand les participants recevront les rétributions ; et
- si l'octroi est soumis à des conditions, par ex. la réalisation d'une tâche précise ou la satisfaction à des tests de contrôle qualité (par ex. dans le cas d'une étude basée sur un panel en ligne).

Les chercheurs doivent également s'assurer que les rétributions sont proportionnées et qu'elles ne constituent pas, ni ne sont assimilées à, de la corruption. Les rétributions doivent être appropriées vis-à-vis de l'audience et de la nature du projet de recherche. Par exemple, si le projet de recherche en ligne porte sur les habitudes en matière de conduite, il serait inapproprié d'offrir des boissons alcoolisées comme rétribution.

Les chercheurs doivent s'assurer que les données collectées dans le but de remettre les rétributions ne sont pas utilisées à toute autre fin, par ex. pour la constitution d'une base de données. Ils ne doivent pas transmettre des informations permettant d'identifier les participants recueillies dans le cadre du processus de rétribution aux clients (y compris les clients internes si la recherche est menée au sein d'un département de recherche chez le client) et/ou toute autre tierce partie, sans l'autorisation explicite des participants.

Les chercheurs doivent être conscients des lois et réglementations locales concernant les rétributions, par exemple dans certains pays :

- L'utilisation de rétributions et/ou d'offres de réductions fournies par les clients, qui exigeraient de la part des participants de dépenser de l'argent afin de recevoir la rétribution (par exemple des réductions de prix sur des biens et services pour lesquelles les participants auraient à s'acquitter du solde pour obtenir l'avantage) est interdite pour les projets de recherche en ligne, puisque ce type d'activité relève du marketing direct

[3] Ceci fait l'objet d'une obligation légale dans certains pays, y compris tous les États membres de l'UE (Union européenne), l'Argentine, l'Australie, le Canada, la Nouvelle-Zélande et les États-Unis (pour les chercheurs qui participent à la Sphère de sécurité convenue entre les États-Unis et l'UE).

(puisque les rétributions et remises fournies par les clients sont considérées comme une forme de promotion client).

- Les rétributions doivent être d'une nature spécifique (par ex. non monétaire).

Dans le cas de projets de recherche en ligne transfrontaliers menés dans plusieurs pays, le processus pour l'offre de rétributions doit respecter toutes les lois pertinentes dans tous les pays impliqués.

3.6.1 Concours et tirages au sort gratuits (aussi appelés loteries)

Les concours et tirages au sort gratuits sont une forme de rétribution particulièrement populaire dans le cadre de la recherche en ligne. Lorsqu'ils en font usage, les chercheurs doivent se conformer aux lois et réglementations locales en vigueur, qui peuvent varier selon les pays, et être conscients des risques importants liés à l'utilisation de cette approche sans en avoir la connaissance détaillée nécessaire, par exemple dans certains pays :

- Il ne doit pas être demandé aux participants de faire quoi que ce soit d'autre que d'accepter de participer aux projets de recherche en ligne pour avoir le droit de participer à un tirage au sort ou un concours gratuits. Il ne peut donc leur être demandé de fournir des réponses à des questions d'enquête, de compléter des enquêtes, etc. pouvant faire partie d'un projet de recherche, en particulier lorsque des quantités de données disproportionnées sont fournies par l'individu, puisque cela peut être considéré comme un participant à « transfert de la valeur monétaire ». Dans de tels cas, cela serait considéré comme un besoin de payer pour participer et le tirage deviendrait une loterie payante soumise à des contrôles réglementaires.

- Un certain niveau de compétence peut être exigé pour participer aux tirages au sort/concours gratuits afin que les participants puissent être ainsi qualifiés, par ex. en posant une question exigeant certaines connaissances tout en restant relativement facile (par ex. Qui est le Président des États-Unis ?), avant que la participation ne soit acceptée.

- Si les participants ne terminent pas les activités ou les projets de recherche, la participation au tirage au sort ou au concours ne peut pas leur être refusée.

Les chercheurs ne doivent pas refuser de remettre les prix des tirages au sort/concours sauf si les participants n'ont clairement pas répondu aux critères énoncés dans les règles régissant le tirage au sort/le concours gratuits (par ex. les règles interdisant la participation au tirage aux membres de la famille du personnel responsable de l'organisation du tirage au sort ou du concours).

Les chercheurs doivent s'assurer que toutes les informations pertinentes concernant le tirage au sort/le concours gratuits sont clairement communiquées aux participants au moment où le consentement est demandé. Les exigences spécifiques varient selon les pays mais comprennent des informations telles que :

- la date limite de participation ;

- la nature du prix ;

- si un équivalent monétaire peut être remis pour remplacer le prix ;

- comment et quand les gagnants seront notifiés des résultats ;

- comment et quand les gagnants et les résultats seront annoncés ;

- les critères de qualification et de disqualification ; et
- les autres moyens de participation.

Toutes les règles doivent être claires et sans ambiguïté, afin d'être faciles à comprendre et non trompeuses pour les participants. Il en va ainsi pour les chances de gagner, la valeur des prix proposés, etc. En outre :

- De telles règles ne doivent pas être déraisonnables et/ou exagérément restrictives.
- Les chercheurs doivent clairement établir une distinction entre les cadeaux offerts à tous les participants au tirage au sort/au concours gratuits, et les prix offerts aux gagnants.
- Les chercheurs doivent s'assurer que plusieurs moyens de participation gratuits sont proposés pour tous les tirages au sort/concours gratuits et que les chances de gagner sont identiques quelle que soit la forme de participation.
- Les chercheurs doivent s'assurer que les gagnants des tirages au sort/concours gratuits sont sélectionnés d'une manière garantissant un respect des lois du hasard. Le processus par lequel les gagnants sont sélectionnés doit être accompagné d'un processus de vérification clair, et tout tirage doit être indépendant. Dans certains pays, des observateurs indépendants peuvent être requis, afin de garantir que tous les participants aient une chance égale de gagner.
- Enfin, les chercheurs doivent s'assurer que les clients sont conscients de leurs responsabilités et potentielles responsabilités pour tout tirage au sort/concours gratuits organisé en leur nom. Les chercheurs doivent discuter avec les clients des approches à suivre pour alléger ces responsabilités (par ex. en incluant une clause d'indemnisation en cas de responsabilité et vis-à-vis de tiers).

Les chercheurs doivent toujours consulter les directives nationales pertinentes avant une telle entreprise.

4 CLIENTS : RELATIONS ET RESPONSABILITÉS

4.1 Sous-traitance

Les chercheurs doivent informer les clients, avant le commencement du projet, lorsqu'une partie quelconque du projet doit être sous-traitée à une entité en dehors de l'organisation du chercheur. Sur demande, l'identité du sous-traitant quel qu'il soit doit être révélée aux clients.

Lorsque l'identité d'un sous-traitant utilisé pour obtenir un échantillon peut légitimement être considérée comme une information protégée, le fournisseur d'échantillons doit fournir :

- une description du type de sources d'échantillons à utiliser ; et
- une estimation du pourcentage de l'échantillon qui devrait provenir de panels et de sources hors panels.

Les chercheurs doivent également s'assurer que toute donnée personnelle partagée avec un sous-traitant se limite au nécessaire pour réaliser la ou les tâches sous-traitées ; que le sous-traitant applique les procédures nécessaires pour la sécurité des données afin de protéger les données ; et que les responsabilités du sous-traitant en matière de protection des données sont clairement documentées et acceptées.

4.2 Protéger les données personnelles

Les chercheurs doivent veiller à ce que l'identité personnelle des participants au projet de recherche ne soit pas révélée aux clients. Sauf dans le cas où les lois et/ou réglementations

en matière de confidentialité en vigueur font l'objet d'exigences plus strictes, le chercheur est autorisé à communiquer les informations personnelles identifiables du participant au client, sous réserve des conditions suivantes :

- le participant a donné son consentement explicite ;
- la finalité est la recherche exclusivement ; et
- aucune activité marketing ou commerciale ne sera adressée au participant du fait qu'il ait fourni ces informations.

En outre, il est essentiel que les chercheurs obtiennent de leurs clients une garantie écrite concernant le fait que le client ne tentera pas d'identifier les participants, sauf si les conditions ci-dessus sont réunies.

4.3 Transparence, déformation et correction des erreurs

Tous les projets de recherche doivent faire l'objet d'une documentation et de rapports précis, transparents et objectifs. Si des erreurs sont découvertes après la livraison, le client doit immédiatement en être informé et des corrections doivent être effectuées sur-le-champ.

Pour en savoir plus sur les exigences en matière de reporting, se référer au point 6 - Qualité méthodologique, plus loin dans ce document.

5 GRAND PUBLIC : RELATIONS ET RESPONSABILITÉS

5.1 Maintenir la confiance du public

Les chercheurs doivent vérifier que les échantillons fournis par les fournisseurs d'échantillons ou leurs clients ne sont constitués que d'individus comprenant qu'ils sont susceptibles de recevoir un e-mail ou un SMS sollicitant leur participation à un projet de recherche. D'autres technologies de messagerie, telles que les notifications d'applications mobiles peuvent avoir des caractéristiques et capacités semblables aux SMS. Cf. point 3.5 pour plus de détails.

5.2 Publier les résultats

Lorsqu'un client prévoit de publier les résultats d'un projet de recherche, le client comme le chercheur ont la responsabilité de garantir que les résultats publiés ne sont pas trompeurs. Ainsi, les clients sont fortement encouragés à consulter le chercheur quant à la forme et au contenu des résultats publiés.

Les chercheurs doivent également être préparés à mettre à disposition, sur demande, des informations techniques suffisantes pour évaluer la validité des résultats publiés. Cela comprend toute information pertinente concernant le contexte de l'étude, la source de l'échantillon, la méthode de collecte des données, la formulation de toute question utilisée, la pondération qui a été utilisée le cas échéant, et tout tableau ou autre résultat analytique faisant l'objet d'un rapport dans le document publié.

Les chercheurs ne doivent pas accepter que leur nom soit associé à la divulgation des conclusions d'un projet d'étude de marché, sauf si ces conclusions sont étayées de manière adéquate par les données.

6 QUALITÉ MÉTHODOLOGIQUE

Si les utilisateurs du projet de recherche en ligne ont la certitude que les résultats correspondent à la finalité, les chercheurs doivent alors mettre à la disposition de ces utilisateurs les informations appropriées concernant la façon dont le projet de recherche a été mené, y compris en ce qui concerne les restrictions méthodologiques qui peuvent mener

à des conclusions qui ne seront pas compatibles avec les données. Ces informations devraient inclure :

- la taille, la source et la gestion de l'échantillon ;
- la conception et la sélection de l'échantillon ;
- la méthode de collecte des données ;
- tout nettoyage de données, toute pondération ou tout ajustement post-terrain ayant pu être effectués ;
- en cas de recherche en ligne dans les pays où l'accès à Internet est limité, les mesures prises pour s'assurer que les résultats de la recherche représentent la population cible de l'étude.

Un ensemble minimum d'exigences figure ci-après. Pour en savoir plus, consultez la directive ESOMAR/GRBN sur la qualité des échantillons en ligne.

6.1 Source et gestion de l'échantillon

Les catégories principales de sources d'échantillon en ligne sont :

- les panels en ligne : un fournisseur d'échantillons a développé un panel ou des panels desquels est tiré un échantillon ;
- les échantillons aléatoires ou dynamiques : tirés d'une source de trafic sur Internet ;
- les échantillons en listes : tels que les listes de clients, les membres d'une association professionnelle, les étudiants d'une école particulière, etc.

Dans chaque cas, le fournisseur d'échantillons doit être préparé à communiquer au chercheur les détails concernant la façon dont l'échantillon a été recruté ainsi qu'une description du cadre d'échantillonnage et la mesure dans laquelle l'échantillon couvre la population cible qu'il est censé représenter. (Par exemple, si l'échantillon désigné correspond au groupe « NatRep », la définition précise de NatRep utilisée pour cet échantillon, ainsi que les groupes démographiques, géographiques ou autres qui sont susceptibles d'être sous-représentés dans l'échantillon, doivent être fournis.) En outre, les chercheurs doivent rapporter les taux d'achèvement et d'interruption, ainsi que les taux de réponse lorsque cela est approprié (par ex. dans le cas d'échantillons en listes) afin de pouvoir évaluer la déformation potentielle liée aux non-réponses.

Le fournisseur d'échantillons doit également être préparé à divulguer les informations relatives aux procédures utilisées pour garantir la qualité des réponses données et des données collectées. Cela comprend :

- les mesures prises pour valider les sources de l'échantillon ;
- les procédures utilisées pour attirer de potentiels participants aux panels, communautés ou listes ;
- les procédures de nettoyage et de mise à jour ;
- la surveillance de la performance quant au remplissage individuel des enquêtes ou les contrôles de qualité pour minimiser le satisficing ou la fraude, ainsi que les mesures prises si un tel comportement est détecté ;

- les procédures de soutien des participants ;
- la façon dont les rétributions sont remises ;
- si et comment de nouvelles sources ont été intégrées au cadre d'échantillonnage ;
- et toute procédure mise en place pour maximiser l'uniformité des échantillons pour les projets de suivi.

6.2 Sélection et conception de l'échantillon

Afin de garantir que les entretiens complétés représentent la population cible et les objectifs du projet de recherche, le chercheur doit documenter tous les quotas ou critères ciblés utilisés dans le cadre de la sélection de l'échantillon, y compris concernant le panachage des sources d'échantillons, l'utilisation de technologies de routage d'échantillons, et les rétributions offertes aux participants.

6.3 Collecte de données

Les chercheurs doivent également faire part à l'utilisateur de la recherche de la façon dont les données ont été recueillies. Si un questionnaire a été utilisé, ces informations devraient comprendre :

- la longueur moyenne ou médiane du questionnaire ;
- la formulation de toutes les questions et tout filtre ou toute instruction pour le participant ;
- les dates de commencement et d'arrêt de la collecte de données ;
- si le questionnaire a été conçu de manière à être compatible avec les smartphones ou les tablettes, et si cela n'est pas le cas, si ces individus ont été exclus de l'échantillon, ou ont participé à une enquête non optimisée pour leur appareil ; et
- tout besoin de prendre des mesures particulières comme télécharger un logiciel ou partager des informations sensibles ou des données personnelles.

6.4 Nettoyage et pondération des données

Le chercheur doit documenter la façon dont les données ont été nettoyées ; si des entretiens terminés ont été retirés des données et pourquoi, et toute information concernant la pondération ou d'autres ajustements. Si des techniques d'imputation sont utilisées, il doit clairement être expliqué quelles variables ont été imputées, dans quelle mesure, et quelles méthodes d'imputation ont été utilisées.

7 RECOMMANDATIONS SUPPLÉMENTAIRES

7.1 Recueillir des données auprès d'enfants

Recueillir des données auprès d'enfants exige d'obtenir la permission d'un parent ou tuteur légal de l'enfant. Les réglementations nationales définissant l'âge à partir duquel l'obtention de cette permission n'est plus nécessaire varie considérablement. Les chercheurs doivent consulter les lois nationales et les codes d'auto-réglementation en vigueur dans les juridictions où les données seront recueillies, afin de déterminer lorsque la permission parentale est requise, ou lorsque les sensibilités culturelles nécessitent un traitement particulier.

Lors du premier contact avec un potentiel participant qui a de grandes chances d'être un enfant, les chercheurs doivent demander l'âge de la personne avant de recueillir toute autre donnée personnelle. Si l'âge donné se trouve en dessous de l'âge de majorité convenu à

l'échelle nationale, l'enfant ne doit pas être invité à fournir d'autres données personnelles avant d'avoir obtenu la permission nécessaire. Le chercheur peut demander à l'enfant de fournir les coordonnées de ses parents ou de son tuteur légal afin que la permission puisse être demandée.

Lorsqu'il demande la permission, le chercheur doit fournir suffisamment d'informations à propos de la nature du projet de recherche afin de permettre au parent ou au tuteur légal de prendre une décision éclairée quant à la participation de l'enfant. Cela comprend :

- le nom et les coordonnées du chercheur/de l'organisation menant la recherche ;
- la nature des données qui doivent être recueillies auprès de l'enfant ;
- une explication de la façon dont les données seront utilisées ;
- une explication des raisons pour lesquelles il a été demandé à l'enfant de participer ainsi que les avantages probables ou impacts potentiels ;
- une description de la procédure pour donner et vérifier le consentement ; et
- une demande des coordonnées d'un parent ou tuteur légal pour la vérification du consentement.

Le chercheur doit également enregistrer l'identité de l'adulte responsable et son lien avec l'enfant.

Il est recommandé aux parents de maintenir l'identité de leurs enfants confidentielle durant leur participation à l'enquête après qu'ils aient accepté de participer à l'enquête, et si nécessaire, d'être prêts à les assister et à les aider à compléter l'enquête.

Une attention particulière doit être portée au sujet de la recherche (y compris des éléments importants tels que des sujets sensibles qui pourraient perturber le jeune participant ou ses parents) ainsi qu'à la conception du questionnaire (adapté aux caractéristiques spécifiques de l'enfant (âge, niveau de compréhension), informer/mentionner à la fois au parent/tuteur légal et à l'enfant qu'il n'est pas obligatoire de répondre à certaines questions, etc.).

L'autorisation préalable d'un parent ou d'un tuteur légal n'est pas nécessaire pour :

- recueillir l'adresse e-mail d'un enfant ou d'un parent seulement afin d'avertir quant à la collecte de données et pour demander l'autorisation ; ou
- recueillir l'âge d'un enfant à des fins de présélection et d'exclusion. Si cette présélection mène à la décision que l'enfant est éligible pour un entretien, la permission doit alors être requise auprès du parent ou du tuteur légal afin de poursuivre avec l'entretien.

7.2 Identification en ligne et technologies de suivi

Un certain nombre de technologies utilisées dans le cadre d'activités marketing en ligne, telles que le suivi en ligne, ont une utilité valable dans la recherche. L'utilisation de ces technologies dans la recherche est une forme de collecte de données passive qui comprend habituellement :

- l'amélioration de l'intégrité des échantillons en ligne ;
- la prévention de la fraude ; ou

- les applications de recherche, notamment à des fins de calcul de l'audience en ligne, de mesure de contenu et de test publicitaire. Dans ces cas ainsi que dans tout cas semblable, le consentement du participant est requis.

7.2.1 Les technologies et exigences spécifiques à utiliser dans la recherche

Ces dernières comprennent :

- les cookies ;
- les objets partagés localement (également appelés cookies Flash) ;
- les pixels espions ; et
- les empreintes numériques et les identifiants d'appareils.

Certaines de ces technologies étant également utilisées à des fins de marketing comme pour le ciblage comportemental en ligne, leur utilisation fait désormais l'objet d'une surveillance rapprochée de la part des législateurs, des organes de réglementation et d'associations de protection de la vie privée, préoccupés par le risque de voir les activités en ligne des individus surveillées à leur insu.

Dans la mesure du possible, un consentement doit être obtenu concernant la manière dont les données personnelles seront collectées, utilisées et rapportées. Cela est particulièrement important lorsque le chercheur demande à un participant à un projet de recherche de télécharger un logiciel sur son appareil. Les agents actifs ne peuvent être utilisés que sur consentement explicite du participant.

Sauf consentement direct ou autre accord existant (tel que les conditions d'utilisation) :

- les données ne doivent être rapportées ou partagées que sous forme agrégée et un contrat doit être conclu avec le destinataire des données dans le cadre duquel ce dernier accepte de ne pas tenter de ré-identifier les individus (cf. point 4.2) ;
- les données personnelles ne doivent jamais être partagées avec un tiers quelconque (y compris les clients) ; et
- les données doivent être rendues anonymes lorsqu'elles ne sont plus nécessaires et si ce processus est impossible, les données doivent être sécurisées en utilisant les bonnes pratiques admises.

Lorsque des technologies de suivi en ligne et d'identification sont utilisées à des fins de recherche, elles doivent exclusivement être utilisées à des fins de recherche et les principes majeurs s'appliquant aux études de marché doivent être respectés (cf. point 3.1 pour en savoir plus) En outre, les chercheurs doivent se soumettre à l'ensemble des lois, réglementations et règles de conduite professionnelles en vigueur.

7.3 Recherche sur mobile

De manière générale, les études de marché sur mobile sont considérées comme une méthode distincte de recherche en ligne, tel qu'expliqué dans la présente Directive. ESOMAR et GRBN ont tout deux publié des directives spécifiques relatives aux mobiles.

Toutefois, une part considérable des participants contactés pour des projets de recherche en ligne choisissent de répondre en utilisant un appareil mobile tel qu'un smartphone ou une tablette. Ainsi, les chercheurs doivent prendre en compte les limites des smartphones (par ex. taille de l'écran et vitesse de téléchargement) lorsqu'ils conçoivent leurs enquêtes en ligne.

7.4 Recherche sur les réseaux sociaux

L'évolution des réseaux sociaux ces dernières années a changé la façon dont des centaines de millions de personnes partagent des informations à leur sujet à travers le monde. Les consommateurs génèrent aujourd'hui de plus en plus leur propre contenu sur Internet. Cela a créé de nouvelles opportunités pour les chercheurs d'observer, d'interagir et de recueillir des informations. De nombreuses techniques ont d'ores et déjà été développées pour profiter des réseaux sociaux, comme les panels communautaires, les communautés en ligne pour les études de marché, le crowdsourcing, la co-création, la « netnographie » les analyses web et de blogs. Il est en outre probable que de nombreuses autres se développent à l'avenir puisque Internet est en évolution constante.

Les chercheurs doivent respecter les mêmes principes éthiques et professionnels fondamentaux qui régissent les projets de recherche en face à face, par e-mail ou par téléphone.

Les données issues des réseaux sociaux comprennent souvent des données personnelles identifiables. De nombreuses réglementations ont été développées dans ce domaine avant qu'il ne soit possible pour une personne de communiquer avec plusieurs sur des plateformes en ligne accessibles à tous. Des mises à jour des lois sur la confidentialité et la protection des données sont toujours en cours et sont souvent en décalage avec des changements de pratiques qui sont désormais largement acceptées.

Néanmoins, les chercheurs doivent consulter les réglementations locales et codes de secteur susceptibles d'exister dans les juridictions où le projet de recherche doit être mené. Pour en savoir plus, consultez le point 3.2.1.

7.5 Nouvelles formes de données personnelles

Les chercheurs doivent convenir que les photographies ainsi que les enregistrements audio et vidéo sont des données personnelles et doivent être traités comme telles. Lorsqu'une image numérique contient le visage d'un individu, clairement visible de telle manière que cela permette à l'individu d'être identifié, cette image est considérée comme donnée personnelle. Ainsi, toutes les photographies et tous les enregistrements audio et vidéo réunis, traités et stockés dans le cadre d'un projet de recherche doivent être traités comme des données personnelles et protégés en conséquence. Ils ne peuvent être partagés avec un client ou utilisateur de recherche que si le participant donne son accord, et uniquement à des fins de recherche. Toute information ayant été convenablement rendue anonyme (comme grâce à une technologie de pixellisation ou de modification de voix), afin que personne ne puisse être personnellement identifié, peut être partagée avec un client ou un utilisateur du projet de recherche.

Consultez la checklist ESOMAR sur la protection des données pour en savoir plus.

7.6 Recherche Business-to-business

Un nombre important de projets de recherche impliquent la collecte de données auprès d'entités juridiques telles que les entreprises, les écoles et les organisations à but non lucratif. De tels projets de recherche impliquent souvent la collecte d'informations à propos de l'entité telles que le montant des recettes, le nombre d'employés, le secteur d'affaires, l'emplacement, etc.

Dans tous ces cas, les organisations participantes ont droit au même niveau de protection contre la divulgation d'identité dans le cadre du reporting que celui accordé aux individus dans d'autres formes de recherche.

Il est important de noter que de nombreuses lois sur la protection des données nationales considèrent l'intitulé de poste ainsi que les coordonnées professionnelles d'un individu comme des données personnelles. Certaines lois sur la protection des données vont encore plus loin en couvrant les personnes physiques et morales (par ex. les individus et les entités

juridiques). Toutefois, les entités juridiques n'ont aucun droit d'accès légal à leurs données, tels que les participants aux projets de recherche.

7.7 Stockage sur le cloud

La décision de stocker des données personnelles sur le cloud doit faire l'objet d'une soigneuse réflexion. Les chercheurs doivent évaluer les contrôles de sécurité du fournisseur de service de stockage sur cloud ainsi que ses conditions générales. Ils doivent être prêts à mettre en œuvre des mesures de contrôle complémentaires lorsque celles du fournisseur ne sont pas suffisantes. Par exemple, les chercheurs devraient chiffrer les données personnelles lors de leurs transferts (vers/depuis le cloud) ainsi que lorsqu'elles ne sont pas utilisées (stockées sur les serveurs du fournisseur de cloud).

Les chercheurs doivent également vérifier les lieux physiques où les données personnelles sont stockées afin de déterminer si le recours au stockage sur le cloud constitue un transfert transfrontalier. Si des données personnelles doivent être transférées d'une juridiction à une autre, le transfert doit respecter les exigences en matière de protection des données à la fois dans la juridiction d'origine et de destination. Le chercheur doit ainsi prendre en considération et comprendre toutes les lois et réglementations nationales et locales en vigueur pour décider des dispositions appropriées.

Les chercheurs doivent sérieusement se poser la question de savoir s'ils doivent placer les données personnelles dans un cloud privée plutôt que dans un cloud public. Dans un cloud privé, le matériel dédié est assigné à la société du chercheur et ce dernier sait en permanence à quel endroit les données personnelles se trouvent.

Au contraire, dans un cloud public, les données peuvent être placées dans deux centres de données ou plus ou dans deux pays ou continents et plus, ce qui peut entraîner des problèmes de conformité, à la fois vis-à-vis des exigences applicables en vertu des lois sur la protection des données et des contrats conclus avec les contrôleurs de données qui spécifient à quel endroit les données personnelles doivent être placées (cf. Checklist ESOMAR sur la protection des données pour en savoir plus).

Enfin, les chercheurs pourraient également envisager de souscrire une police d'assurance contre les cyber-risques. Un grand nombre de fournisseurs de services de stockage sur le cloud offrent de très faibles indemnités lorsqu'ils causent des atteintes à la sécurité et que les données personnelles sont compromises. Cela signifie que la société du chercheur assumerait un risque important quant aux dommages et pertes financiers découlant de graves atteintes à la sécurité causant des dommages aux individus affectés.

7.8 Anonymisation et pseudonymisation

Un élément essentiel de la responsabilité du chercheur en matière de protection des données est de supprimer tout caractère identifiant des données avant la transmission à un client ou même au grand public. L'anonymisation est une protection qui implique soit la suppression soit la modification des éléments identifiants afin de présenter les données sous une forme qui ne permette pas d'identifier les individus. Cela peut par exemple être fait en floutant les images afin de masquer les visages, ou en rapportant les résultats sous forme de statistiques agrégées, de manière à ce qu'il ne soit plus possible d'identifier un individu particulier.

La pseudonymisation implique de modifier les données personnelles afin qu'il soit toujours possible de distinguer les individus dans un fichier de données, par exemple en utilisant un identifiant unique, ou des algorithmes de hachage tout en conservant séparément leurs données personnelles à des fins de vérification.

Lorsqu'ils emploient de telles techniques, les chercheurs devraient consulter les lois nationales en vigueur et les codes d'auto-réglementation pour déterminer quels éléments doivent être supprimés afin de respecter la norme légale concernant l'anonymisation et la pseudonymisation pour de telles données.

7.9 Utilisation d'identifiants statiques et dynamiques

Historiquement l'utilisation d'identifiants statiques de participants aux projets de recherche (identifiants statiques) a été utilisée parmi les clients de recherche et les fournisseurs d'échantillons afin de mieux contrôler et attribuer les participants aux projets de recherche aux études spécifiques, à la fois longitudinales et ad hoc. Cette technique a permis de consolider les informations détenues à propos de chaque participant et est devenue une approche permettant de garantir que les individus ne participent qu'une fois à une même étude longitudinale et que les périodes d'exclusion aux enquêtes soient respectées. Outre le fait d'améliorer le contrôle des périodes d'exclusion et la sélection des échantillons, et la possibilité d'identifier précisément les participants individuels aux projets de recherche, certains chercheurs emploient également les identifiants statiques afin de faciliter leur analyse des données.

L'utilisation d'identifiants dynamiques (identifiants variables pour chaque utilisation) a été soutenue par certains fournisseurs d'échantillons comme un moyen d'aider à protéger l'identité de membres individuels, de prévenir ou de réduire le risque que des clients sans scrupules utilisent les données des participants aux projets de recherche ainsi que les autres données collectées (données périphériques) durant la session d'entretien avec les participants afin d'obtenir une perspective supplémentaire ou pour essayer de révéler la véritable identité d'un participant.

Les chercheurs devraient veiller à choisir le bon type d'identifiant et à équilibrer les enjeux de confidentialité et de qualité de la recherche pour leur étude. Des dispositions légales et contractuelles devraient être appliquées afin de contrôler la collecte et l'utilisation des informations générées par l'étude en respectant les limites contractuelles dictées par les accords convenus entre toutes les parties (participant à la recherche, fournisseur d'échantillon, chercheur, client final).

7.10 Utilisation et contrôle des données périphériques

Il est recommandé de soumettre l'utilisation des données périphériques à des accords légaux mutuels entre le fournisseur d'échantillons et le client afin de guider, de limiter et de protéger la collecte, l'utilisation et le transfert ultérieur de ces données dans le processus de recherche subséquent.

7.11 Pratiques inacceptables

Vous trouverez ci-dessous une liste des pratiques inacceptables que les chercheurs doivent strictement interdire ou empêcher. On considère que les chercheurs utilisent des logiciels espions lorsqu'ils font usage de l'une ou plusieurs des pratiques suivantes :

- télécharger des logiciels sans obtenir l'accord du participant ;
- télécharger des logiciels sans indiquer et révéler intégralement, clairement et de manière concise et bien visible les types d'informations qui seront recueillis, ainsi que la façon dont ces informations pourront être exploitées ;
- utiliser des espions de clavier sans obtenir le consentement éclairé du participant ;
- installer des logiciels qui modifient les paramètres de l'ordinateur du participant au-delà de ce qui est nécessaire pour le déroulement du projet de recherche ;
- installer des logiciels qui désactivent les logiciels anti-espion, antivirus ou antispam, ou prenant le contrôle voire piratant l'ordinateur ou l'appareil du participant ;

- ne pas déployer tous les efforts possibles pour s'assurer que le logiciel n'entre pas en conflit avec les principaux systèmes d'exploitation et n'entraîne pas un fonctionnement erratique ou inattendu des autres logiciels installés ;

- installer des logiciels cachés dans d'autres logiciels qui peuvent être téléchargés ou qui sont difficiles à désinstaller ; ou qui produisent du contenu publicitaire, à l'exception des logiciels prévus pour l'évaluation publicitaire ;

- installer des mises à jour de logiciels sans en avertir les utilisateurs ni donner au participant l'opportunité de s'y opposer ;

- changer la nature des technologies d'identification et de suivi sans en avertir l'utilisateur ;

- ne pas avertir l'utilisateur des changements apportés aux pratiques de confidentialité lors de la mise à jour de logiciels ;

- suivre le contenu des e-mails du participant ;

- si le navigateur du participant est paramétré en mode privé, suivre le comportement sans consentement éclairé ; et

- si le participant se trouve sur un site web protégé par un protocole de sécurisation (par ex. un site SSL), recueillir des données personnelles sans consentement éclairé.

8 RÉFÉRENCES

- Checklist ESOMAR sur la protection des données

- Directive ESOMAR/GRBN sur la qualité des échantillons en ligne

- Global Research Business Network

- Code international ICC/ESOMAR des études de marché et d'opinion

- ISO 20252:2012 – Études de marché, études sociales et d'opinion

- ISO 26362:2009 – « Access panels » pour les études de marché, études sociales et d'opinion

- ISO 27001 -- Technologie de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences

9 L'ÉQUIPE DU PROJET

- Reg Baker, Coprésident, Consultant auprès du Professional Standards Committee d'ESOMAR, Marketing Research Institute International

- Peter Milla, Coprésident, Consultant technique chez CASRO, Peter Milla Consulting

- Mario Callegaro, Chercheur scientifique senior, Google

- Melanie Courtright, Vice-présidente exécutive - Services clients internationaux, Research Now

- Brian Fine, Président, Quality Online Research
- Phillipe Guilbert, Directeur général, Toluna
- Debrah Harding, Directrice générale, Market Research Society
- Kathy Joe, Directrice des normes internationales et des affaires gouvernementales, ESOMAR
- Jackie Lorch, Vice-président - Gestion internationale des connaissances, SSI
- Bruno Paro, Directeur général, Netquest
- Efrain Ribeiro, Directeur de recherche, Lightspeed Research
- Alina Serbanica, Vice-présidente senior - Services interactifs, Ipsos