Contextualité des questions de privacy dans l'utilisation de services interactifs et conséquences pour la conception

Myriam Fréjus, Julien Guibourdenche, Dominique Martini

Contextualité des questions de privacy dans l'utilisation de services interactifs et conséquences pour la conception

The Contextuality of Privacy Issues in Interactive Services, and its Consequences for Design

FREJUS, Myriam
Electricité de France Recherche et Développement

GUIBOURDENCHE, Julien
AKTEN - Université de Genève

MARTINI, Dominique
ITG

ABSTRACT

We are interested in how issues relating to privacy and confidentiality are incorporated when using interactive services. Two smart home services based on the use of data from "smart" electricity meters have been evaluated to establish the guarantees and forms of interaction necessary for their appropriation. We show that, given the contextual, dynamic and social nature of privacy, normative responses such as those promoted by the regulator (predefinition of sensitive data, prior to use consent, privacy as the default setting) are insufficient. As mentioned in previous works, the design choices must promote as components of the systems the user control of data throughout the interaction, as well as transparency of the data, processing and actors. However, our results highlight an important dimension not previously addressed: the need to adopt a temporal and diachronic vision of privacy and to broaden the question of interaction beyond use by considering the life cycle of the service and of the relationship with its suppliers.

Nous nous intéressons à la façon dont les questions de vie privée et de sa préservation s'instancient dans l'utilisation de services interactifs. Deux services relatifs à l'habitat et basés sur l'exploitation de données issues de compteurs électriques « intelligents » ont été évalués pour établir les garanties et formes d'interactions nécessaires à leur appropriation. Nous montrons que, compte tenu de la nature contextuelle, dynamique et sociale de la privacy, les réponses normatives telles que celles promues par le législateur (prédéfinition des données sensibles, consentement a priori, privacy intégrée seulement au stade de la conception du système) sont insuffisantes. Comme cela a pu être évoqué dans des travaux antérieurs, les choix de conception doivent favoriser la maîtrise des données dans l'interaction en proposant des moyens d'actions et une transparence des données, traitements et acteurs, en tant que composantes des systèmes. Toutefois, nos résultats mettent en exergue une dimension importante non traitée jusqu'alors : la nécessité d'adopter une vision temporelle et diachronique de la privacy, pour élargir la question de l'interaction au-delà de l'utilisation en considérant la durée de vie du service et de la relation avec ses fournisseurs.

IHM '23, April 03–06, 2023, TROYES, France

ACM ISBN 978-1-4503-9824-4/23/04…$15.00
https://doi.org/10.1145/3583961.3583970

CCS CONCEPTS

• **Human and societal aspects of security and privacy**; • **Empirical studies in HCI**; • **Human-centered computing**;

KEYWORDS

Privacy, Design, Consent, Situated analysis, Lived experience, Context, Personal data
Mots-clés additionnels : Privacité, Conception, Consentement, Analyse située, Expérience vécue, Contexte, Données personnelles

ACM Reference Format:
FREJUS, Myriam, GUIBOURDENCHE, Julien, and MARTINI, Dominique. 2023. Contextualité des questions de privacy dans l'utilisation de services interactifs et conséquences pour la conception: The Contextuality of Privacy Issues in Interactive Services, and its Consequences for Design. In *IHM '23: Proceedings of the 34th Conference on l'Interaction Humain-Machine (IHM '23), April 03–06, 2023, TROYES, France.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3583961.3583970

1 INTRODUCTION

Les questions de vie privée constituent un objet majeur d'attention tant populaire qu'académique [5, 12, 25, 52, 64]. De tous temps s'est posée la question du rapport entre ce qui doit rester du domaine privé et ce qui doit être visible de l'ensemble de la société, mais les débats et développements théoriques à ce sujet se sont surtout construits en lien avec les développements technologiques [63]. Le numérique provoque un déplacement des rapports public/privé en changeant les façons de percevoir et d'agir ainsi que les structures sociales et les droits individuels en leur sein [39]. Ainsi, en s'élargissant bien au-delà de la bureautique pour intégrer la technologie dans les objets du quotidien, l'informatique pervasive a pu être considérée ces trente dernières années comme profondément intrusive et susceptible de générer de nouveaux problèmes de privacy [10, 36] ; en cause l'accumulation des données personnelles liée aux nouvelles possibilités de capture, de stockage et de transmission, couplée à la potentielle invisibilité des dispositifs numériques dans l'espace et à leur manque de contrôle par l'Humain. La privacy est ainsi considérée comme le principal frein au développement de l'informatique ubiquitaire [36]. Les récents développements de l'intelligence artificielle [66] viennent compléter les craintes en ce qu'ils s'appuient non seulement sur le traitement de grandes masses de données mais aussi sur des capacités d'apprentissage capables de générer connaissances et inférences sur les personnes. Ces données acquièrent une permanence en tant qu'enregistrements numériques et peuvent être interrogées efficacement voire commercialisées, avec des conséquences sur la vie privée des utilisateurs (par exemple, révéler des informations sur les activités, les comportements

ou les déplacements des personnes). La commercialisation des données, même si elle se traduit en services pour les consommateurs, marque aussi leur perte de contrôle sur leurs données : [37] parlent « d'asymétrie de l'information », en ce que les individus savent moins ce que deviennent leurs données que les entreprises qui les exploitent avec leurs propres objectifs à l'esprit. En contre-poids aux promesses et à l'enthousiasme engendrés par les avancées technologiques, de nombreuses voix s'élèvent donc quant aux risques de détournement des données, pouvant aller jusqu'à des fins de contrôle, de contrainte ou de sanctions des individus, groupes sociaux ou États [44]. Ces dispositifs et technologies renouvellent d'autant les questions éthiques [21, 32].

1.1 La privacy : une notion contextuelle, dynamique et sociale

Si l'importance grandissante de ces questions ne fait plus de doute, un manque de consensus quant à ce qu'elles recoupent apparait toutefois [9] : la privacy ou, selon sa déclinaison francisée la privacité[1], recouvre différentes dimensions et se réfère principalement au droit des individus ou des organisations à garder le contrôle de l'accès à l'information et aux individus (ou à la manière dont ils peuvent le perdre) [25]. Elle résulte de phénomènes différents, incluant la solitude (le droit d'être laissé seul) [63], la confidentialité (le droit de contrôler ses propres informations) [64] et l'autonomie (le droit de contrôler la présentation de soi) [34, 40]. Pour certains, la privacité est « *l'accès que d'autres ont à vous grâce à l'information, à l'attention et à la proximité physique* » [33] ; pour d'autres, c'est « *la condition dans laquelle d'autres personnes sont privées d'accès à certaines informations sur vous* » [50]. Notons que ces définitions restent très inspirées des pratiques du monde occidental, majoritairement individuelles, alors que dans d'autres régions et cultures le groupe joue un rôle différent et les frontières de l'information sont différentes.

Comme l'indique Solove [54], la privacité est le produit de normes, d'activités et de protections juridiques. Elle n'est pas une chose, mais un ensemble de nombreuses choses distinctes mais liées. Aucune de ces activités n'est intrinsèquement mauvaise. Selon la théorie de l'intégrité contextuelle de Nissenbaum [44], il n'existe pas de normes universelles de protection de la vie privée, mais elles sont distinctes pour chaque situation et aident à maintenir l'intégrité contextuelle. Celle-ci décrit un état souhaitable vers lequel les individus tendent, en gardant les informations perçues comme privées selon le contexte. [41] montrent que les questions de vie privée sont liées aux activités réalisées. [25] rappellent sa dimension fondamentalement collective et sociale : « *Privacy is not simply a way that information is managed but how social relations are managed* » (p. 327). La privacité, comme la sécurité, sont des réalisations pratiques et continues, constamment produites et révisées, collectivement [25]. Ils dénoncent aussi la vision utilitariste et soutiennent que la vie privée ne peut pas être considérée uniquement comme une rationalité économique, où des renseignements personnels sont fournis en échange d'un service ou d'une valeur sociale. Les pratiques d'information sont des compréhensions collectivement reproduites des façons dont les informations devraient être partagées, gérées et dissimulées [4, 28].

[1]Nous utiliserons indifféremment ces deux termes.

1.2 Respecter la privacy : une question de conception plus que de prescription

En réponse aux risques pesant sur la vie privée, les législateurs tentent d'imposer certaines règles éthiques et juridiques pour cadrer la conception des dispositifs (comme l'AI Act à l'échelle européenne en cours d'élaboration qui exige « transparence et maîtrise humaine des systèmes »). Si en matière de conception nombre de questions ne sont pas nouvelles, force est de constater que les réglementations qui se mettent en place à visée d'éthique n'intègrent pas les points de vue humains et situés ni ne définissent ce qu'est un système transparent et maitrisable.

En écho, la privacité et la sécurité constituent des aspects clés de l'Interaction Humain Machine (IHM) et suscitent trois principaux types de travaux : l'étude des pratiques de privacité/sécurité, de l'utilisabilité des technologies de privacité/sécurité et la conception de nouveaux mécanismes utilisateurs de gestion de la vie privée et de la sécurité [2, 4, 13, 20, 29, 65].

L'étude de Urban et al [61] a révélé que 62% des utilisateurs d'Internet se sont peu inquiétés de leurs données personnelles lorsqu'ils avaient la possibilité de voir les conditions détaillées et les termes de la politique de confidentialité. Les utilisateurs sont plus confiants lorsqu'ils savent que leurs informations ne sont pas stockées mais supprimées [56] et inversement limitent la divulgation d'informations lorsqu'elles peuvent être transférées à des tiers, ou quand un réseau sans fil est utilisé [38]. On constate toutefois des décalages entre l'expression de besoins de confidentialité et les pratiques réelles [9], la valeur perçue prenant souvent le pas sur les besoins de privacy [19]. Les individus ne connaissent pas exactement la nature et la destination des données partagées. De ce fait, la modification des paramètres de confidentialité intervient lorsque les utilisateurs sont confrontés à de réels problèmes plutôt qu'en anticipation. L'acceptation des nouveaux systèmes dépend donc aussi de leur capacité à rendre accessible les éléments liés à la préservation de la vie privée [43].

En réponse à ces problématiques, des principes ont été définis pour la prise en compte des questions de privacité dans la conception [10, 21, 51]. Ces principes consistent à :

- Définir des feedbacks dont les utilisateurs doivent disposer à propos du recueil, de l'utilisation et du partage des données, ainsi que les motifs associés à l'utilisation de leurs informations [7] ;
- Définir des modes de contrôle à leur fournir ;
- Établir un guide pour les concepteurs où chaque élément fournit un type spécifique de préoccupation sur lequel les concepteurs doivent se concentrer [53] ;
- Préconiser une minimisation des données [60], etc.

Les principes de « privacy by design » (PbD) [15] intègrent aussi la prise en compte de l'utilisateur et pointent la nécessité de proposer des moyens de contrôle et d'information, au moment où ils sont les plus judicieux et compréhensibles par les utilisateurs (contrairement à la demande habituellement constatée de consentement à la connexion, résultante des demandes réglementaires). Le PbD exige de la transparence et une posture centrée utilisateur. Cette dernière est surtout traitée en proposant des notices, ou des options « user friendly » telles qu'avoir accès aux informations personnelles utilisées ou établir des préférences. Le paramétrage est considéré

comme un moyen de donner le contrôle en édictant ses préférences, de façon permanente dans le temps [15, p.50]. Le regroupement des informations dans un « privacy center » centralisant toutes les politiques de confidentialité d'un opérateur de services est plébiscité. Le PbD a le mérite de rappeler l'importance d'avoir une démarche centrée utilisateur et de travailler l'interface et l'utilisabilité des systèmes pour faciliter l'accès aux informations relatives à la privacy. L'opérationnalisation de ces principes reste toutefois ambigüe. En effet, le PbD préconise aussi qu'aucune action ne soit nécessaire de la part de l'utilisateur pour protéger sa privacité, celle-ci étant intégrée au système automatiquement, par défaut. De plus, si les concepteurs doivent intégrer des « options conviviales » par défaut dans les produits, les modalités de « convivialité » considérées comme telles par les utilisateurs dans leur expérience ne sont pas précisées [47]. Et surtout, dans quelles circonstances les données doivent-elles être privées par défaut ? [9] déplore que la privacy soit souvent considérée en IHM comme un concept quantifiable plutôt qu'un vécu. Cela renvoie davantage à la protection des données comme prescription de ce qui peut être légalement partagé ou non, plutôt qu'à la privacité personnelle où chacun peut maîtriser son flux d'information. D'ailleurs, dans un monde fait de capteurs pervasifs et d'objets connectés, la démarche majoritaire consistant à notifier / choisir parait insuffisante, voire susceptible de freiner l'activité des personnes [1, 62].

Palen & Dourish [46] montrent que la maîtrise de la privacité n'est pas statique ou basée sur des règles et que ce ne sont pas les paramètres de privacité eux-mêmes contenus dans la technologie qui sont importants mais plutôt comment celle-ci s'intègre dans les pratiques de gestion de la privacité. Pour preuve la difficile gestion des paramétrages figés, là où le partage de flux d'informations est contextuel : les utilisateurs préfèrent se censurer plutôt que paramétrer des listes [9]. Aussi, plutôt que de se focaliser sur le partage, DePaula et al. [22] réinscrivent la gestion de la privacité dans les pratiques collectives d'information et remettent en cause la séparation entre configuration et action qui caractérise les systèmes interactifs pour gérer la sécurité et la privacy. Comme l'utilisabilité, la privacy ne peut être une caractéristique ajoutée in fine voire limitée à l'interface. Il s'agit d'une composante intrinsèque du système.

La gestion de la vie privée est ainsi une question de conception des systèmes et de l'interaction entre les gens et ces systèmes qui prélèvent des données, gèrent des flux et permettent de partager. La nature contextuelle de la privacy renvoie au point de vue des personnes en situation, évoluant compte tenu de leurs activités. Au contraire, une définition extrinsèque du contexte centrée sur des éléments de l'environnement (i.e. localisation, identités des personnes, technologies présentes [3, 24]), comme on a pu le considérer dans les systèmes sensibles au contexte, renvoie à une version figée pour le système et non aux contextes humains. Les réponses à construire pour maîtriser sa privacy doivent donc intégrer une vision contextuelle basée sur l'analyse de la façon dont la privacité s'instancie dans les activités individuelles et collectives en situation.

1.3 Connaître la privacité : une question d'analyse située des activités humaines et d'appropriation des technologies

Si les questions de vie privée s'inscrivent dans un contexte social, temporel et collectif, il importe de les documenter en tenant compte de ces aspects pour penser la conception. Barkhuus [9] dénonce le manque d'ancrage terrain des études utilisateurs au profit de la détermination de types d'informations supposées partageables selon le cadre social considéré. Il importe de dépasser les notions de partage et de normes, y compris contextuelles, lorsqu'elles renvoient à des concepts pré-définis plus qu'à des critères localement et variablement définis selon les activités et préoccupations en cours.

Considérer la privacité comme une action pratique consiste à s'intéresser à ce que les gens font, plus qu'aux échanges d'information abstraits, et selon leur propre subjectivité. Cette contextualité de la privacité renvoie à l'analyse située des activités humaines et de l'appropriation des technologies. On entend par là de prendre pour objet non pas l'acceptabilité sociale et les opinions et critères a priori portés sur la protection de la vie privée mais plutôt d'étudier la relation entre l'Humain et les technologies dans son contexte social, historique et organisationnel de réalisation [27, 49, 55, 57], là où les questions de vie privée sont un critère parmi d'autres en jeu. L'analyse située des activités humaines telle que pratiquée en ergonomie francophone permet d'élaborer des modèles d'activité resituant la technologie et son appropriation dans ses cadres de mise en œuvre réels, eux-mêmes non statiques, évoluant et se développant dans le temps en lien avec l'histoire individuelle et collective [11, 45, 58]. On aborde ainsi la technologie par ce qu'elle fait (ou défait) et ce qu'elle apporte (ou enlève), et non pour ce qu'elle est ou ce que l'on suppose qu'elle sera (vision déterministe et/ou probabiliste de la privacité). Ce qui revient *in fine* à étudier les conditions d'acceptation des nouvelles pratiques associées à ces technologies. Selon cette approche orientée activité, chaque activité étant située, elle ne peut être dissociée du contexte d'où elle émerge. Aussi, méthodologiquement, on s'intéresse à l'expérience réelle, au vécu et aux pratiques effectives des individus au contact de ces technologies, documentés du point de vue des acteurs [14, 59] et resitués dans leur cadre socio-technique d'émergence, i.e. au-delà de l'interaction seule.

1.4 Contexte et objectifs de la recherche

Dans le secteur énergétique, le déploiement des smart grids soulève de nombreuses questions et polémiques relatives à l'exploitation des données issues des compteurs intelligents et constitue un important sujet de préoccupations compte tenu de ce que ces informations peuvent donner à voir des sphères privées et domestiques. Dans le même temps, les smart grids, couplées à des appareils connectés et distribués sont des opportunités de nouveaux services dans les habitats à travers le développement d'habitats « intelligents » (smart home) et/ou pour la relation avec les clients (suivis et analyses de consommations, adaptation tarifaire, etc.) [30].

La vie privée et sa préservation constituent un sujet déterminant dans l'appropriation de la smart home et plus généralement dans la vie domestique. Elle motive en elle-même l'usage de certains équipements (comme les volets par exemple, [48]). Pour le maintien

à domicile, domaine phare de développement de l'habitat « intelligent » [23, 42], la confiance et le respect de la vie privée sont essentiels pour les personnes âgées, rappelant leur besoin d'intimité et leur volonté de ne partager des informations que de manière sélective [6, 26]. Inversement, les personnes peuvent rechercher la capture d'informations si elle garantit un meilleur fonctionnement du système, comme c'est le cas d'usagers du système de gestion du chauffage Nest qui se forcent à passer régulièrement devant son capteur pour que leur présence dans le logement soit bien prise en compte dans la programmation automatique [67].

Cavoukian et al. [16] ont décliné le « privacy by design » au domaine énergétique pour proposer un modèle conceptuel (Smart-Privacy) destiné à préserver la privacy tout en garantissant les pleines fonctions de la smart grid. Ces principes restent succincts et consistent principalement en une limitation des données exploitées et en la possibilité pour les utilisateurs de déclarer des préférences quant à leur exploitation, accéder aux informations et les corriger éventuellement. [16] pointent toutefois que les implications de la smart grid en termes de privacy ne sont pas bien connues et doivent encore être évaluées.

La prise en compte des contextes dans l'habitat et la gestion de la privacy afférente est un sujet complexe et difficile en raison de la nature des activités humaines et des possibilités des technologies : les dispositifs peinent à prendre en compte les activités, d'autant qu'elles ont une dimension collective et ne sont pas forcément reliées à un individu seul ; elles s'inscrivent dans une distribution spatiale et temporelle rendant difficile toute délimitation. Et enfin, il y a une asymétrie entre les contextes humains (propres à l'individu, son contexte social, son histoire, ses finalités et préoccupations dans l'activité en cours) et ce qui peut être capté par un système, qui ne peut être qu'une vision appauvrie si ce n'est erronée [35].

Ces limitations quant aux difficultés à développer une approche contextuelle de la privacy dans l'habitat, couplées à la méfiance et aux polémiques associées au comptage énergétique intelligent impliquent de fait de donner des garanties aux clients. Les questions de respect de leur vie privée doivent être bien prises en compte dans les nouveaux services qui découlent des possibilités offertes par la smart grid, ce qui sous-entend que les garanties et formes d'interactions proposées s'inscrivent bien dans les pratiques et attentes en termes de gestion.

C'est dans ce contexte que nous avons été sollicités pour évaluer deux types de services, relatifs à l'habitat et basés sur l'exploitation de données de comptage :

- Un service de suivi d'activités quotidiennes de leurs parents vivant seuls par des proches à distance
- Un parcours web de consentement à l'utilisation de données personnelles de consommation d'énergie par un Tiers sur internet.

Ces deux études nous intéressent en ce qu'elles apportent des éclairages complémentaires sur la question de l'instanciation de la privacy dans la conception : la première concerne des personnes âgées, et par extension des données, considérées par la législation sur la privacy comme sensibles car relatives à des personnes catégorisables comme vulnérables. L'évaluation porte sur la durée de vie du service, ce qui permet d'identifier des freins potentiels dès la souscription et non au moment de l'utilisation seule. Il mobilise un réseau de proches à qui la personne âgée donne à voir une part de sa vie domestique ce qui permet de situer ce service dans son tissu relationnel et social.

Le second service porte plus sur l'interaction et la matérialisation dans l'interface des dimensions relatives à la privacy (parcours de consentement, informations sur l'exploitation) mobilisant des acteurs et des données énergétiques sujets à débats sur la scène médiatique et réglementaire. Il s'inscrit directement dans les craintes qui ont pu être évoquées dans la littérature de commercialisation à des Tiers de données personnelles.

Ces deux études ont consisté à analyser en situations réelle (étude 1) ou réaliste (étude 2) l'appropriation de ces services pour voir comment les questions de préservation de la vie privée s'y instanciaient. Notre hypothèse étant que la conception de solutions de maîtrise et de gestion de la privacité doit s'appuyer sur l'analyse de l'émergence et des conséquences des questions de privacité dans la réalisation des activités humaines, étudiées en contexte et du point de vue des acteurs. Considérer ainsi les questions de vie privée et les pratiques d'information soulève selon nous deux questions clés que nous souhaitons adresser dans cet article. Une question technologique tout d'abord : comment concevoir des systèmes sociotechniques à même de respecter et, mieux, de favoriser les pratiques recherchées par les individus ? Cette visée de conception suppose de répondre préalablement à une question de recherche empirique : comment la privacité s'instancie-t-elle dans les activités individuelles et collectives en situation ?

Nous allons dans la partie suivante présenter les deux études et leurs résultats. Puis nous discuterons de ceux-ci pour identifier les caractéristiques clés de l'interaction à même de répondre aux besoins de privacy et les positionnerons en regard aux éléments de littérature présentés précédemment.

2 DEUX ETUDES DE L'APPROPRIATION SITUEE DE DISPOSITIFS/SERVICES A BASE DE DONNEES PERSONNELLES

2.1 Étude 1 : Suivi d'activités de leurs parents vivant seuls par des proches

2.1.1 Recueil et méthodologie. Cette étude est en fait constituée de deux études terrain correspondant à deux phases distinctes de développement d'un service de suivi à distance de l'activité de personnes vivant seules à domicile. À partir de l'analyse des consommations électriques et de la mise en œuvre d'algorithmes d'apprentissage et de reconnaissance, ce service propose à une personne âgée vivant seule et à ses proches de visualiser sur un smartphone les heures de lever/coucher, de prise de repas ou encore les présences/absences du logement. L'idée est de permettre à des membres de la famille d'une personne âgée (souvent éloignés) de veiller sur elle à distance et éventuellement de détecter des dysfonctionnements relevant d'une fragilité qui s'installe ou d'un problème visible dans les rythmes de vie.

La première phase d'étude (étude 1A) s'est adressée à des participants volontaires d'une expérimentation de ce service [31] : 7 proches (35-60 ans) et 6 parents (retraités de 74 à 86 ans).

L'évaluation est réalisée au domicile de chaque parent ou, pour les proches, sur leur lieu de travail, un lieu neutre (restaurant par ex.)

ou au domicile selon leur préférence. Elle comporte deux phases : un entretien portant sur leur histoire et vie quotidienne, leurs attentes et projection de services utiles et une remise en situation sur l'expérience vécue avec l'application les semaines précédentes ; et des observations de l'utilisation in vivo (avec verbalisations simultanées sur l'utilité et la facilité d'usage). Les entretiens sont enregistrés et les utilisations filmées afin de transcrire et exploiter des verbatims et séquences d'interaction.

La seconde phase (étude 1B) a concerné 19 participants :13 « proches » de 24 à 62 ans et 6 « parents » de 53 à 77 ans. Les proches de 50/60 ans se projettent aussi spontanément comme futurs « parents ». L'évaluation a eu lieu par observations directes à domicile de l'utilisation d'une seconde version de l'application mobile maquettée sous adobe XD suite aux retours de la phase 1 et avec entretiens. L'évaluation sur mobile comportait plusieurs séquences : une découverte libre qui permettait d'observer comment l'utilisateur prenait en main l'application spontanément ; une mise en situation d'utilisation par scénario qui permettait de comprendre la facilité d'utilisation et de navigation ; un retour précis sur les scénarios permettant de détailler les raisonnements et expériences vécues à certains moments lors des scénarios ; un retour général sur la découverte et l'usage de la maquette mobile par l'utilisateur, permettant d'apprécier l'utilité des fonctionnalités, les attentes et besoins à prendre en compte, la clarté des libellés et si l'application respectaient la vie privée du parent. Enfin des alternatives d'écrans pour mobile ont été présentées de manière à comprendre les préférences des participants et les raisons de ces préférences.

L'analyse a donc porté à la fois sur l'ensemble des verbatims transcrits intégralement et sur les séquences dynamiques d'activité filmées. Les questions relatives à la privacy ont été majoritairement exprimées pendant l'usage ou les entretiens et exploitées via les verbatims, en rapport ou non avec des fonctionnalités présentes/absentes dans l'application.

2.1.2 Résultats (restreints par le filtre vie privée). Les personnes âgées dont l'activité peut être suivie par des Tiers n'ont pas exprimé de freins majeurs quant à cette « surveillance ». Même si ce retour est restreint à ceux qui ont accepté d'y souscrire, ceux-ci jugent le service peu intrusif. L'atteinte à la vie privée est jugée de manière **relative** à d'autres formes de surveillance ou d'intrusion :

- Sociale, par les voisins par exemple « je préfère ce petit fil ténu par [l'énergéticien] que la surveillance par mes voisins. Les retraités ça passe son temps à espionner » (parent, étude 1A)
- Par les professionnels de santé : « le contrôle dans la profession médicale c'est quotidien donc ça me choque pas » (parent, étude 1A).

Ce sont les proches eux-mêmes qui craignent d'être intrusifs et se demandent comment aborder le service et gérer le fait d'avoir accès à certaines informations. La question de l'intrusion des proches dans la vie privée de leur parent s'est trouvée réglée de deux façons : tout d'abord, la souscription au service s'est faite entre des proches et des parents inscrits dans une relation de confiance, au sein d'un cercle social jugé acceptable. Ensuite, cette confiance a été confortée au moment de la présentation du service du proche envers le parent. Les proches expriment ainsi des attentes en termes d'aides à la présentation du service au parent. Face à leur gêne liée au risque d'intrusion, la personne suivie affiche plutôt de l'indifférence, elle aussi justifiée par les relations de confiance existantes : « *Moi ça me rassure, ça me réconforte. Si elle (la proche) ça la dérange pas c'est déjà une bonne chose de pouvoir voir si ça va bien* » (parent, étude 1A). Cette surveillance est même jugée positive en ce qu'elle va générer du lien social et des contacts avec les proches jugés trop rares. Elle s'inscrit en fait dans **une relation de confiance construite antérieurement et confortée par la matérialisation tangible du service**, l'ensemble relevant d'une démarche globale de bienveillance : « *Ils (voisins jeunes amis) trouvent ça intrusif. Mais je leur ai dit : mais mon voisin de palier est bien pire ! (rires) (. . .) Puis la deuxième fois je leur ai montré le papier que mon gendre m'avait envoyé (impression des écrans) et là ça allait, ça a concrétisé, ça fait des repères. C'est comme les volets à l'époque on voyait si les personnes étaient actives ou non en regardant si les volets étaient fermés ou non. C'est prendre soin les uns des autres, c'est pas intrusif* » (parent, étude 1A).

Lorsqu'il y a des réactions négatives face à la présentation du service, celles-ci dénoncent surtout la surveillance (du flicage, big brother. . .). Mais ces réactions a priori peuvent être suivies **d'évolutions positives** à la découverte concrète du service, des apports ou des enjeux, notamment s'il y a une plus-value perceptible. Il faut aussi qu'il y ait une justification au recueil de certaines données pour le service : « *Je suis prêt à laisser [l'énergéticien] accéder à des nouvelles données si un service est rendu. Le médical et la banque plutôt non, mais l'eau par exemple oui. Mais pourquoi [l'énergéticien] prendrait les données bancaires ?* » (proche étude 1B).

Les principaux freins proviennent d'expériences passées négatives concernant le contrôle de ses données par l'utilisateur et une **anticipation négative** quant à la sécurité, aux conditions de stockage et à l'utilisation non contrôlée par des Tiers : « *Une fois j'ai autorisé PayPal pour eBay mais ils prenaient pour tout après. Du coup j'ai supprimé eBay. C'est traître parce que une fois que tu as cliqué tu peux plus revenir en arrière. T'as pas le droit à l'erreur. C'est peut-être fait exprès ceci dit* » (proche étude 1B). Ces réticences sont la marque de trois préoccupations majeures : pouvoir garder la main sur ses données, pouvoir les gérer contextuellement et que le service et l'utilisation des données soient transparents.

Pouvoir garder la main signifie de gérer les droits des parties prenantes, de déclarer des proches ou d'établir des configurations de relations selon les liens de confiance et de bienveillance. Pour certains utilisateurs (qu'ils soient parents ou proches), la privacy doit pouvoir être gérée en partie **dynamiquement**, ce qui renvoie à des besoins fonctionnels sur l'application : pouvoir choisir le type et niveau de détail que traitent le compteur électrique intelligent et l'application, pouvoir facilement arrêter ou mettre en pause l'enregistrement des données : « *Il faudrait un bouton pour couper l'application si la personne veut pendant un moment dire stop »; « moi je désinstallerais l'appli en fait. Vous savez ces moments où on n'a pas envie de voir qui que ce soit, où on veut être dans sa bulle. C'est une question de liberté en fait. Pour les deux, proches et parent* » (proches étude 1A). Enfin, les besoins exprimés de transparence du service ne sont pas restreints à l'utilisation : savoir ce que fait l'application et en quoi consiste le service (dès le premier contact), savoir quelles données sont recueillies, savoir à qui et à quoi servent les données, quel est mon pouvoir de contrôle et de décision mais

aussi matérialiser ces informations tout au long du parcours des clients.

D'autres éléments jouent sur les attentes de respect de la vie privée, en fonction des personnes (plus ou moins technophiles) ou des données : si elles sont déjà partagées (par exemple les données de comptage électrique avec l'énergéticien) ou selon leur maille et leur nature. L'acceptation de l'exploitation des données reste ainsi très personnelle, certaines pouvant même être jugées déjà trop disséminées (données médicales par exemple). En fait, ces critères ne sont pas figés et les normes de partage évoluent : « *Les données santé sont déjà sur internet avec AMELI etc... Mettre sur la TV revient à mettre la TV sur PC : tout le monde est habitué. Ma mère fait des achats sur internet, c'est plus normal qu'avant* » (proche étude 1B).

Ainsi, nous pouvons nous demander ce qui est réellement sensible : la donnée ou son contexte d'utilisation ? Dans ces études, les données ne sont pas jugées « sensibles » par nature mais il existe des attentes sur l'utilité (un service utile et de qualité doit être fourni), la sécurité (respect du Règlement Général sur la Protection des Données (RGPD), sécurité et éthique de l'utilisation, non revente), et la confiance (garder la main, pas de « dark pattern » dans l'interaction) : « *Les données ok si c'est terriblement encadré. Hors de question de poser les données à Tataouine. Les conditions doivent être très claires et la RGPD aussi. Il faut qu'il y ait une honnêteté complète qu'on m'explique pourquoi, pour quel usage. Et à tout moment je dois être capable de dire ce que j'en fais, si je veux revenir en arrière, etc.* » (proche, étude 1B). C'est donc un cadre global de confiance et de maîtrise qui procure les conditions sociales, techniques et réglementaires nécessaires pour accepter le partage d'une donnée, que ce soit avec un fournisseur de service ou avec un proche. Et ce cadre est évolutif : en se nourrissant de faits antérieurs, d'anticipations, de comparaisons, il dépasse l'utilisation proprement dite.

2.2 Étude 2 : évaluation d'un parcours web de consentement à l'utilisation de données personnelles par un Tiers

2.2.1 Recueil et méthodologie. Cette étude consiste en une évaluation utilisateur d'une maquette de parcours client en ligne réalisée par un Distributeur d'énergie. La maquette matérialise un parcours où, depuis des sites Tiers qui pour leur service utiliseraient des données de consommations énergétiques recueillies par le distributeur d'énergie, l'utilisateur, disposant d'un compteur communiquant, serait renvoyé vers son espace client chez le Distributeur pour recueillir son consentement à l'utilisation des données par ce Tiers. Ce passage par le site du Distributeur doit aussi lui permettre d'obtenir l'ensemble des informations nécessaires à son accord : données qu'il va partager, durée du partage, du consentement, détails sur les données, explications pédagogiques, mais aussi révocation des accords donnés, etc. Le parcours web a été conçu par les équipes digitales du « Distributeur », sur la base de ce que les concepteurs estimaient être pertinent, juridiquement autorisé et techniquement possible. Nous sommes sollicités après coup pour le tester en situation réaliste d'usage et tester l'idée d'une gestion centralisée des consentements sur le site du Distributeur.

Ainsi, 12 clients particuliers du Distributeur (7 hommes et 5 femmes) ont été mis en situation réaliste d'utilisation pour évaluer le parcours client proposé, et leur compréhension de la notion de Tiers et de consentement. Différentes options de résiliation d'enregistrement et de collecte de données sur une maquette du site Distributeur ont aussi été testées auprès de 8 de ces 12 clients. L'utilisation des prototypes de sites était filmée et précédée d'entretiens individuels. L'analyse a porté sur ces entretiens retranscrits. L'ensemble des vidéos a été visionné et certaines séquences d'interaction jugées illustratives des problèmes soulevés ou problématiques ont été plus particulièrement analysées (transcrites et découpées en catégories de problèmes/besoins).

2.2.2 Résultats (restreints par le filtre vie privée). La notion de Tiers est globalement comprise mais suscite surtout des craintes d'un usage commercial des données personnelles pour vendre autre chose que ce qui était prévu (crainte des spams). La nécessité de passer un accord, le consentement, est comprise. Toutefois, ce consentement repose sur la confiance elle-même dépendante de plusieurs facteurs qui ne sont **pas forcément liés au contexte spécifique d'utilisation** : pouvoir définir l'usage de ses données (pour un objectif précis, une durée définie, un Tiers unique) ; savoir comment résilier ; connaître l'entreprise.

Ainsi, l'entreprise Tiers évoquée dans le prototype n'étant pas connue des utilisateurs n'a pas suscité suffisamment de confiance pour que les participants souhaitent s'inscrire ou utilisent leurs identifiants du Distributeur pour s'y connecter. Les utilisateurs ne sont pas non plus rassurés quant à la fiabilité de ce Tiers : ils expriment en anticipation des craintes en termes d'usage des données ou de protection de ces données une fois acquises. Un travail d'explication et de réassurance doit être fournit par le Tiers mais aussi par le Distributeur qui doit également s'engager en termes de responsabilités et de garanties. Les mauvaises expériences passées (avec des partenaires commerciaux du Distributeur) plaident en sa défaveur. On voit donc que la confiance doit être construite pour l'ensemble des parties prenantes et le fait de connaitre le Distributeur (et reconnaitre son logo) n'est pas suffisant. Pour faire autorité, la réputation et la marque sont nécessaires mais pas suffisantes.

Qui dit Tiers et fournisseur de données dit questionnements sur l'articulation des deux et sur le rôle du Distributeur : quel rôle(s) le Distributeur garde-t-il ? Passer par le Tiers en fait-il mon interlocuteur unique ? Que me garantit le Distributeur ? Est-ce lui qui fournit les données au Tiers ou est-ce le Tiers qui accède aux données du Distributeur ? Naissent des doutes quant à la procédure de transfert de données : « *« je consens et je partage » les termes laissent penser que [le Tiers] va accéder à mes données, donc aller les chercher. Ce n'est pas l'idée que c'est [le Distributeur] qui transmet* ». Ces questions marquent les **interrogations des clients quant à la nouvelle organisation proposée et à son propre positionnement en son sein** ; elles montrent le **besoin de comprendre les nouveaux flux d'informations proposés et leurs limites**, prévues ou à définir par le client.

Ces inquiétudes relèvent aussi d'une **anticipation** des difficultés à venir pour reprendre son consentement et de la peur de manquer de moyens d'agir pour reprendre la main et gérer ses propres données ; le manque d'information vient en renforcement de la méfiance comme possible volonté de cacher des choses. Les clients

se projettent en anticipation de la fin du service et veulent connaitre les traitements prévus de leurs données : ce que les données deviennent, ce qui se passe à la fin de la période couverte par le service, la persistance des garanties de non-transmission vers d'autres Tiers. L'utilisateur ne sait pas si des actions sont attendues de sa part (doit-il arrêter le transfert des données lui-même ?) et doute de pouvoir les réaliser car il ne sait pas comment retrouver les informations sur la résiliation qui lui ont été présentées lors du consentement ni quelles informations mettre dans le mail de résiliation (coordonnées, n° client, n° du point de livraison (PDL) ?) Comment être assuré du résultat ?

L'interface et les informations fournies sont cruciales pour la compréhension et l'acceptation du service et les maquettes évaluées ne répondaient pas aux exigences. Les utilisateurs ont en effet cherché dans le site différents renseignements : quelle est la responsabilité de la société Tiers ? Où se trouve le détail de l'engagement du Tiers ? Et pourquoi n'a-t-il pas été présenté (nécessité d'aller dans les Conditions Générales d'Utilisation (CGU)) ? Mais ces informations sont manquantes dans le prototype ou ne sont pas présentées au bon moment du parcours du client ou de la bonne façon (à dérouler et non affichées d'emblée). Elles sont considérées comme constitutives du contrat proposé et leur absence génère de la méfiance.

Les termes utilisés dans l'interface ont aussi aggravé ces doutes ; par exemple, l'évocation de « mon usage d'électricité » comme dénomination des données « *laisse à penser que l'entreprise peut accéder à ce que je fais, c'est intrusif. Il s'agit de « ma consommation » et pas de « mon usage* » ! ». Aux termes maladroits s'ajoute un manque de cohérence : ce qui s'appelle « Point de Livraison » pour le Distributeur est appelé « Point d'usage » par le Tiers, évoquant à nouveau le manque d'articulation entre les deux.

Les informations données doivent aussi être cohérentes avec le service promis. Dans le prototype, la durée de recueil des données est jugée incohérente avec le service d'analyse des consommations: soit trop longue « *Pourquoi 4 mois ? [le Tiers] annonce sur son site qu'il peut faire un diagnostic en 7 jours »,* soit trop courte *« 4 mois. . . ce n'est même pas 2 saisons* ». L'absence de justification ne permet pas à l'utilisateur de lever ses craintes.

Le client doit **sentir qu'il maîtrise** : ici s'opposent le fait de donner un consentement, synonyme de passivité, avec le fait de demander un service, dont on définit les contours. Être acteur du service revient à définir les données importantes/utiles voire pouvoir choisir d'envoyer soi-même une extraction de ses données sur une période choisie : « *je veux un accès direct, une synthèse, c'est aujourd'hui que je veux voir ce qui se passe dans ma consommation. Il faudrait pouvoir choisir des périodes passées pour de l'analyse ; un accès aux données sur l'historique et à la demande* ».

Ainsi l'action d'accepter le partage de ses données ne doit pas apparaître comme un « blanc-seing », un partage automatique. L'utilisateur doit disposer en anticipation des informations lui permettant de voir clairement où on se rétracte (lien), les CGU, la durée (justifiée) du consentement, les données concernées (formulées dans les termes du fournisseur de services connu ayant les données et faisant référence pour le client) ; et lui permettant d'agir et de modifier au fil de l'eau. Il faut aussi des moyens de vérification de l'effectivité de la résiliation lui permettant de s'assurer a posteriori que les flux ont bien été stoppés et que ses données ne sont plus exploitées.

Enfin, si l'on s'intéresse généralement à la gestion du consentement du client, il importe tout autant de gérer la non-acceptation. Les utilisateurs veulent connaître les enjeux et conséquences du refus afin de les mettre en balance et accepter, ou non, l'utilisation de leurs données en toute connaissance de cause. Mes données sont-elles perdues si je refuse l'enregistrement pendant une période ? Que se passe-t-il avec les données enregistrées / collectées au préalable de ma résiliation ? Puis-je voir mon historique de données même si, depuis, j'ai refusé l'enregistrement ?

Cette étude nous montre donc toute l'importance dans la conception des systèmes de définir au préalable les informations clés nécessaires et de travailler tant la présentation que l'interaction à même de fournir à l'utilisateur les connaissances nécessaires et lui assurer qu'il conserve la maîtrise de ses données. Mais ces connaissances et cette maîtrise s'inscrivent sur la temporalité du service et pas seulement de l'interaction.

3 DISCUSSION DES RESULTATS

Nos résultats sont en phase avec les travaux antérieurs développés en introduction quant à la nature contextuelle, collective et sociale des questions de privacy. La privacy n'est pas figée et renvoie au contexte d'utilisation vu de l'utilisateur plus qu'à la donnée en elle-même. La qualité « personnelle » de la donnée renvoie à l'autonomie de la personne et à son souhait de garder la main et inscrire l'utilisation de ses données dans une démarche personnelle, voire collective négociée, et évolutive selon le temps, l'espace, le groupe social, ou encore la forme prise par le service.

Une première conséquence de ces résultats est que les réponses normatives telles que celles promues par le législateur (prédéfinition des données sensibles, consentement a priori, privacy intégrée seulement au stade de la conception du système) sont pour cela insuffisantes. La minimisation des données recueillies, leur anonymisation, l'obtention d'un consentement ou le recours à toute règle s'appliquant à la donnée seule répondent à des attentes de garanties mais ne sont pas suffisants pour prendre en compte dans la conception les dimensions que nous venons d'évoquer [51].

La seconde conséquence est donc que les choix de conception doivent favoriser la maîtrise des données dans l'interaction, comme cela a pu être évoqué dans les travaux antérieurs. Comme [22], nous considérons qu'une conception intégratrice des préoccupations contextuelles liées aux questions de vie privée doit être favorisée.

Toutefois, nos données mettent en exergue une dimension importante non traitée jusqu'alors : la nécessité d'adopter une vision temporelle et diachronique de la privacy, allant au-delà de l'utilisation pour considérer la durée de vie du service et de la relation avec ses fournisseurs.

Nous détaillons ces deux dimensions en termes de fonctionnalités et de formes d'interaction à privilégier.

3.1 Donner le pouvoir de maîtriser dynamiquement en situation

La maîtrise des données dans l'interaction repose sur deux piliers : le fait de disposer de moyens d'action et la transparence des données, traitements et acteurs. Il s'agit de penser l'interaction avec le détenteur des données pour lui rendre sa place dans leur gestion.

D'un point de vue fonctionnel, l'utilisateur doit donc pouvoir :

- Gérer les droits des parties prenantes : donner ou reprendre le droit d'exploitation de ses données, déclarer une durée d'autorisation
- Stopper ou mettre en pause le recueil des données (avant, pendant et après l'usage). Ce qui nécessite de disposer des informations de résiliation et des fonctions afférentes
- Configurer des relations : pouvoir configurer qui peut exploiter quelles données
- Définir pour chaque type de données le niveau de détail exploitable (niveau de profondeur de la donnée, maille temporelle, etc.)

Ces fonctionnalités plaident pour un centre de gestion de ses préférences et paramètres de privacy tel que prôné par [17] mais les réponses figées de type paramétrage ou l'assimilation stricte du caractère sensible à la qualité personnelle ne répondent pas aux besoins de gestion en contexte. C'est pourquoi des possibilités d'actions doivent aussi être présentes et déclinées dans l'interface [22] au fil de l'usage.

Ces possibilités de maîtrise reposent également sur une transparence des flux et des traitements susceptibles elle aussi d'inscrire la privacy comme composante intrinsèque du système. L'utilisateur doit ainsi pouvoir savoir en temps réel quelles données sont exploitées (en lien avec ses paramètres et son éventuel refus d'exploitation de certaines données) : l'interface doit faire référence aux données sous-jacentes au service, voire montrer les fonctionnalités rendues impossibles par l'absence de données. Les informations ne doivent pas être cachées ou du moins leur présentation ne doit pas laisser penser qu'il puisse y avoir tromperie ou blocage d'actions. On évitera donc les menus cachés, les contenus enfouis dans des thématiques non spécifiques à la privacy (comme les CGU) ou au fond d'arborescences. Enfin, la confiance sera aussi renforcée si le système parait consistent et cohérent au fil de l'usage (terminologie constante, cohérence entre les fonctions permises et les données demandées par exemple). Les garanties données et les moyens d'agir doivent persister dans le temps.

Cependant, les critères sous-tendant le consentement à l'exploitation des données ne sont eux pas persistants. Non seulement les besoins de maitrise et d'information changent mais ils dépassent aussi le cadre strict de l'utilisation. Les marques d'anticipation, les effets d'expériences antérieures jugées négatives, les demandes d'informations sur les acteurs du service que nous constatons dans nos données impliquent d'adopter une vision temporelle et diachronique de la privacy.

3.2 Adopter une vision temporelle et diachronique de la privacy

Nos résultats montrent que la gestion de la vie privée est une préoccupation qui s'inscrit en actions dans différentes temporalités, en anticipation, pendant l'usage ou après. Elle évolue selon la plus-value perçue, les technologies et les normes de partage, qui elles-mêmes changent concomitamment. Elle est donc temporelle en ce qu'elle évolue dans le temps, et diachronique en ce que cette évolution relève d'un processus dynamique de construction et d'interdépendance entre événements.

Tout d'abord, elle s'inscrit dans un cadre préexistant de relation entre les parties prenantes, source de confiance ou non. Toutefois, même pour des acteurs faisant autorité et crédit, elle n'est en aucun cas systématique. Des garanties doivent donc être données dès la phase de découverte du service :

- Si la privacy relève d'une volonté de maîtriser son propre flux d'information, il importe de montrer ce flux, les traitements opérés et la place de l'utilisateur.
- Les opérateurs du service doivent être présentés
- L'utilisateur doit pouvoir savoir quelles données sont utilisées comment elles sont traitées : calculs, stockage, revente éventuelle, respect des réglementations, RGPD notamment. Les engagements concernent tous les acteurs impliqués dans le service.
- Ses possibilités de contrôle doivent être explicites et tangibles
- Les données demandées doivent être cohérentes avec le service produit (tout comme leur durée d'exploitation). On peut ainsi dire que le consentement d'un utilisateur porte sur la combinaison du service et des données.

L'ensemble de ces informations doivent être visibles pour toute la durée de vie du service pour cet utilisateur, consultables pendant l'utilisation ainsi qu'a priori. Par exemple de la même façon qu'il existe des didacticiels pour présenter les usages possibles d'une application, un didacticiel centré sur les questions de privacy, couplé à un centre de contrôle et à des fonctions de gestion diffuses dans l'application pourraient répondre aux besoins et constituer une déclinaison de la privacy dans la conception de la relation de service. Il faudra aussi que la fin du service (fin d'utilisation / résiliation, échéance de consentement) soit anticipée, ce qui suppose :

- De faire connaître les traitements de données prévus ou non après la fin d'utilisation (exploitation, persistance des garanties)
- Préciser à l'utilisateur son rôle à la résiliation ou après les traitements : doit-il intervenir sur les données ?
- Lui valider / faire un retour sur ses demandes relatives à l'arrêt de l'exploitation des données.

La vision temporelle et diachronique de la gestion de la privacy que nous prônons implique d'élargir la question de l'interaction au-delà de l'utilisation du système numérique à celle du service pour envisager une relation de service centrée privacy : transparente, durable, laissant à l'utilisateur/souscripteur sa part d'autonomie dans ses choix (susceptibles d'évoluer) et son contrôle (qui doit être permanent).

4 CONCLUSION

La gestion de la privacy ne peut être réduite à donner un consentement car elle s'inscrit dans l'exercice de l'autonomie des personnes qui doivent être impliquées en tant qu'actrices du service. Elle relève donc bien d'une question de conception de l'interaction entre les personnes et le service, à différents moments, potentiellement de façon collective, et dans des temporalités qui ne sont pas forcément celles de l'utilisation.

Tenir compte de la contextualité des questions de préservation de la vie privée implique de se référer aux vécus des personnes et à leurs activités, considérées dans leurs contextes sociaux, historiques et technologiques ; ils doivent être documentés pour définir les formes de prise en compte de la privacy dans la conception du service et des dispositifs interactifs.

Différentes questions restent toutefois ouvertes. Tout d'abord, demander le consentement, permettre des contrôles, informer des traitements, etc., constituent autant de perturbations de l'interaction : comment traiter correctement des questions de privacy sans bloquer l'interaction et remettre en cause l'utilisabilité des systèmes ? Les préconisations que nous faisons quant à la transparence, la maîtrise et la temporalité de la gestion de la privacy doivent aussi être enrichies à l'aune d'autres études et modélisations des activités humaines en contexte et à partir d'évaluations d'autres services. De plus, leur concrétisation dans la conception, aux différents stades d'usage du service, doit donner lieu à des travaux spécifiques, en ergonomie et en IHM, centrés sur les besoins humains et non sur les réglementations seules.

REFERENCES

[1] M. Ackerman and L. Cranor, 1999 Privacy critics: UI components to safeguard users' privacy. CHI EA '99: CHI '99 Extended Abstracts on Human Factors in Computing Systems

[2] M. Ackerman, L., Cranor & J. Reagle. 1999. Privacy in e-commerce: Examining user scenarios and privacy preferences. Proceedings of the ACM 1999 Conference on Electronic Commerce. New York: ACM.

[3] M. Ackerman, T. Darrell and D. J. Weitzner .2001 Privacy in Context. Human-Computer Interaction 16(2)

[4] A. Adams and M.A. Sasse. 1999. Users are not the enemy: why users compromise security mechanisms and how to take remedial measures. Commun. ACM, 42(12): 40-46.

[5] P. Agre and M. Rotenberg (Eds.). 1997. Technology and privacy: The new technological landscape. Cambridge, MA: MIT Press.

[6] M. Alaoui, M., Lewkowicz and A. Seffah. 2012. Increasing Elderly Social Relationships Through TV-Based Services. HI'12, January 28–30, 2012, Miami, Florida, USA.

[7] R. Alawadhia and T. Hussain. 2019. A Method Toward Privacy Protection in Context-Aware Environment. Procedia Computer Science 151 (2019) 659–666

[8] S.A. Anderson. 1991. Privacy without the right to privacy. The Monist, Vol. 91, No. 1, pp. 81-107. Oxford University Press

[9] L. Barkhuus. 2012. The Mismeasurement of Privacy: Using Contextual Integrity to Reconsider Privacy in HCI. CHI 2012, May 5–10, 2012, Austin, Texas, USA

[10] V. Bellotti and A. Sellen. 1993. Design for Privacy in Ubiquitous Computing Environments. Proceedings of the Third European Conference on Computer-Supported Cooperative Work, 13-17 September, 1993, Milan, Italy. G. De Michelis, C. Simone and K Schmidt (Editors)

[11] M.E. Bobillier Chaumon and M. Dubois. 2009. L'adoption des technologies en situation professionnelle : quelle articulation possible entre acceptabilité et acceptation ? Travail Humain, 72(4), 355-382.

[12] D. Brin. 1999. The transparent society. New York: Perseus.

[13] Brostoff, S., & Sasse, A. (2000). Are passfaces more usable than passwords? In S. Mc-Donald, Y. Waern, & G. Cockton (Eds.), Proceedings of HCI 2000 Conference on People and Computers XIV–Usability or Else! (pp. 405-424). London: Springer.

[14] B. Cahour, C. Brassac, P., Vermersch, J., Bouraouis, B., Pachoud and P. Salembier. 2007. Étude de l'expérience du sujet pour l'évaluation de nouvelles technologies : l'exemple d'une communication médiée. Revue d'anthropologie des connaissances, vol. 1, 1(1), 85-120.

[15] A. Cavoukian. 2009. Privacy by design: the 7 foundational principles. Information and Privacy Commissioner of Ontario.

[16] A. Cavoukian, J. Polonetsky and C. Wolf. 2010. SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation. IDIS (2010) 3:275–294. DOI 10.1007/s12394-010-0046-y

[17] A. Cavoukian and B. Weiss. 2012. Privacy by Design and User Interfaces: Emerging Design Criteria - Keep it User-Centric (Office of the Information and Privacy Commissioner, Ontario, Canada, June

[18] R. Clarke. 1988. Information Technology and Dataveillance. Commun. ACM 31,5 (May 1988) 498-512

[19] R. Compañó and W. Lusoli. 2010. The Policy Maker's Anguish: Regulating Personal Data Behavior Between Paradoxes and Dilemmas. In Economics of Information Security and Privacy (pp. 169-185). Springer US

[20] L. Cranor and J. Reagle. 1998. Designing a social protocol: Lessons learned from the platform for privacy preferences project. InJ. K. MacKie-Mason, & D. Waterman (Eds.), Telephony, the Internet, and the media. Mahwah, NJ: Lawrence Erlbaum Associates.

[21] G. Danezis, J. Domingo-Ferrer, M. Hansen, J. Hoepman, D. Metayer, R. Tirtea & S. Schiffner. 2014. Privacy and data protection by design-from policy to engineering. ENISA.

[22] R. DePaula, X. Ding, P. Dourish, K. Nies, B. Pillet, D. Redmiles, *et al.* 2005. In the eye of the beholder: A visualization-based approach to information system security. International Journal of Human-Computer Studies, 63, 5-24.

[23] A. Desai and R. Jhaveri. 2017. A review on applications of ambient assisted living. Int. J. Comput. Appl. 176(8), 1–7.

[24] A. K. Dey, P.J. Brown and G. D. Abowd. 1999. Towards a better understanding of context and context-awareness. In Handheld and ubiquitous computing (pp. 304-307). Springer Berlin Heidelberg.

[25] P. Dourish and K. Anderson. 2006. Collective Information Practice: Exploring privacy and security as social and cultural phenomena. Human-Computer Interaction. 21, 319-342.

[26] E. Elias, M.E. Chaumon and M. Vacher. 2018. Methods to Design Home Support for Elders. In J. Zhou and G. Salvendy (Eds.): Human Aspects of ITfor the Aged Population. ITAP. Springer International Publishing AG.

[27] Y. Engeström. 1999. Expansive visibilization of work: an activity-theoretical perspective. Computer-Supported Cooperative Work 8, 63–93.

[28] G. A. Fine and L. Holyfield. 1996. Secrecy, trust, and dangerous leisure: Generating group cohesion in voluntary organizations. Social Psychology Quarterly, 59(1), 22–38.

[29] I. Flechais, M.A. Sasse and S. Hailes. 2003. Bringing security home: A process for developing secure and useable systems. Proceedings of the ACM/SIGSAC New Security Paradigms Workshop (pp. 49-57). New York: ACM.

[30] M. Fréjus. 2019. Élargissement et renouvellement des questions traitées par l'ergonomie dans le domaine du développement durable : retour sur 12 ans de travaux sur les activités domestiques et la maîtrise des consommations énergétiques. Psychologie Française. Volume 64, Issue 2, June 2019, Pages 179-196.

[31] M. Fréjus & J. Guibourdenche 2021. Quantified self for others: lessons learned from the evaluation of a remote monitoring service of the activities of the elderly. In: Ahram, T.Z., Falcão, C.S. (eds) Advances in Usability, User Experience, Wearable and Assistive Technology. AHFE 2021. Lecture Notes in Networks and Systems, vol 275. Springer, Cham.

[32] M. Fréjus, D. Lahoual & M. Gras-Gentiletti 2022. Making Human-AI Interactions Sustainable: 7 Key Questions for a Human-Centered Perspective on AI. In: Francisco Rebelo (eds) Ergonomics In Design. AHFE International Conference. AHFE Open Access, vol 47. AHFE International, USA.

[33] A. Froomkin. 2000. The death of privacy? Stanford Law Rev. 52(5), 1461–1543.

[34] R. Gavison. 1980. Privacy and the limits of the law. Yale Law Journal, 89, 4,21-471.

[35] J. Guibourdenche, J. Vacherand-Revel, M., Fréjus and Y. Haradji. 2015. Analyse de contextes d'activité domestique pour la conception de systèmes diffus énergétiquement efficients. Activités, 12-1.

[36] J. Hong, and J. Landay. 2004. An Architecture for Privacy-Sensitive Ubiquitous Computing. MobiSys'04, June 6–9, 2004, Boston, Massachusetts, USA.

[37] X. Jiang, J.I. Hong and J. A. Landay. 2002. Approximate information flows: Socially-based modeling of privacy in ubiquitous computing. In Ubicomp 2002: ubiquitous computing (pp. 176-193). Springer Berlin Heidelberg

[38] P. Klasnja, S. Consolvo, J. Jung, B.M. Greenstein, L. LeGrand, P. Powledge and D. Wetherall. 2009. When I am on Wi-Fi, I am fearless: privacy concerns and practices in everyday Wi-Fi use. In Proc. of CHI '09. ACM, New York, NY, USA.

[39] T. Matzner and C. Ochs. 2019. Privacy. Internet Policy Review, 8(4). DOI: 10.14763/2019.4.1427

[40] D. Mayer-Schönberger. 2009. Delete: The Virtue of Forgetting in the Digital Age. Princeton University Press, Princeton

[41] F. Mc Creary, A. Zafiroglu & H. Patterson. 2016. The Contextual Complexity of Privacy in Smart Homes and Smart Buildings. In F.F.-H. Nah and C.-H. Tan (Eds.): HCIBGO 2016, Part II, LNCS 9752, pp. 67–78.

[42] J. Nehmer, M., Becker, A., Karshmer and R. Lamm. 2006. Living assistance systems: an ambient intelligence approach. In: Proceedings of the 28th International Conference on Software Engineering, pp. 43–50.

[43] T. Nilsson, A. Crabtree, J. Fische & B. Koleva. 2018. Breaching the Future: Understanding Human Challenges of Autonomous Systems for the Home, July 2018. Rapport DOI: 10.13140/RG.2.2.23719.85920. Project: Future Everyday Interaction with the Autonomous Internet of Things.
[44] H. Nissenbaum. 2004. Privacy as Contextual Integrity. Washington Law Review 79 (30).
[45] W.J. Orlikowski. 2000. Using technology and constituting structures: a practice lens for studying technology in organizations. Organization Science, vol. 11, n°4, pp. 404-428.
[46] L. Palen & P. Dourish. 2003. Unpacking "privacy" for a networked world. Proceedings of the SIGCHI conference on Human factors in computing systems. ACM Press, Ft. Lauderdale, Florida, USA, 129-136.
[47] H. Patterson, A. Zafiroglu & F. McCreary. 2016. Facets: a framework for developing privacy-minded usages. In: Proceedings of CHI 2016.
[48] G. Poizat, M., Fréjus and Y. Haradji. 2013. Domestic ergonomics: contribution to the design of a smart home lighting service. In J. C. Spohrer & L. E. Freund (Eds.), Advances in the human side of service engineering design (pp. 84-93). Boca Raton, FL: CRC Press.
[49] P. Rabardel. 1995. Les hommes et les technologies : Approche cognitive des instruments contemporains. Paris : Armand Colin.
[50] J. Reiman. 1976. Privacy, intimacy, and personhood. Philos. Publ. Aff. 6(1), 26–44.
[51] G. Rostama, A. Bekhradi & B. Yannou. 2017. From privacy by design to design for privacy. International Conference on Engineering Design (ICED), Aug 2017, Vancouver, Canada.
[52] B. Schneier. 2000. Secrets and lies: Digital security in a networked world. New York: Wiley.
[53] D. Solove. 2006. A taxonomy of privacy. Univ. Pennsylvania Law Rev. 154(3), 477–560.
[54] D. Solove. 2008. Understanding privacy. Harvard University Press 2008.
[55] L. Suchman. 1987. Plans and situated actions: The Problem of Human-Machine Communication. New York: Cambridge University Press.
[56] S. Sundar, J. Kim, J. Gambino & M.B. Rosson. 2016. Six ways to enact Privacy by Design: Cognitive heuristics that predict users online information disclosure. Workshop on Bridging the gap between privacy by design and privacy in practice at CHI 16.
[57] J. Theureau. 2003. Course-of-action analysis and course-of-action centered design. Handbook of cognitive task design, pp. 55–81.
[58] J. Theureau. 2011. Appropriations 1, 2 & 3. Communication présentée au Séminaire ErgoIDF, Cnam, Paris, France, Juin.
[59] J. Theureau. 2015. Le cours d'action. L'enaction et l'expérience. Toulouse : Octarès.
[60] E. Toch and Y. Birman. 2018. Towards Behavioral Privacy: How to Understand AI's Privacy Threats in Ubiquitous Computing. UbiComp '18, 931–936.
[61] J. Urban, C.J. Hoofnagle & S. Li. 2012. Mobile phones and privacy. Center for the Study of Law and Society. http://emsoc.be/wp-content/uploads/2012/07/SSRN-id2103405.pdf
[62] R. Warner and R. Sloan. 2013. Beyond notice and choice: privacy, norms, and consent. J. High Technol. Law.
[63] S.D. Warren and L.D. Brandeis. 1890. The Right to Privacy. Harvard Law Review, 4(5), 193–220. doi:10.2307/1321160
[64] A.F Westin. 1967. Privacy and Freedom. New York NY: Atheneum.
[65] A. Whitten and D. Tygar. 1999. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. Proceedings of the Ninth USENIX Security Symposium.
[66] W. Xu. 2019. Toward Human-Centered AI: A Perspective from Human- Computer Interaction. Interactions, july-august, ACM.
[67] R. Yang and M.W. Newman. 2012. Living with an intelligent thermostat: advanced control for heating and cooling systems. Proceedings of the 2012 ACM Conference on Ubiquitous Computing.