Minicursos da X Escola Regional de Informática de Mato Grosso
ISBN: 978-85-7669-487-8
DOI: https://doi.org/10.5753/sbc.4587.8

Capítulo 1

Despertando o olhar para a *Early Privacy*: desafios e recursos para o estabelecimento de privacidade em sistemas computacionais

Deógenes P. da Silva Junior, Patricia Cristiane de Souza

Abstract

Privacy is an important requirement of computer systems in the current context of frequent leakage of users' personal data, as well as the lack of knowledge or control of these users over what data is collected, how it is collected and what actions are taken with that data. Early Privacy is a defense of privacy design that evolves alongside software design, respecting usability and accessibility aspects to ensure that users in their widest diversity can effectively make decisions about their personal information in the technological context. This short course presents a discussion of the Early Privacy concept and current issues of privacy, as well as artifacts to provide designers with the ability to specify and design privacy in their computer system designs.

Resumo

Privacidade é um requisito importante de sistemas computacionais no contexto atual de vazamento frequente de dados pessoais de usuários, bem como da falta de conhecimento ou controle destes usuários sobre quais dados são coletados, como são coletados e quais ações são realizadas com estes dados. A "privacidade desde cedo" (Early Privacy) é uma defesa do projeto de privacidade que evolui juntamente com o projeto de software, respeitando aspectos de usabilidade e acessibilidade para garantir que os usuários em sua maior diversidade possam efetivamente tomar decisões sobre suas informações pessoais no contexto tecnológico. Este minicurso apresenta uma discussão sobre o conceito de Early Privacy e as problemáticas atuais de privacidade, bem como artefatos para munir projetistas com a capacidade de especificar e projetar a privacidade em seus projetos de sistemas computacionais.

1. Introdução

Os serem humanos não apenas mais usam as tecnologias, mas vivem com elas [Sellen et al., 2009]. Deste modo, o design dessas tecnologias se torna um problema complexo que envolve muitas vezes fatores não explícitos, como valores humanos e cultura, que implicam diretamente

ISBN: 978-85-7669-487-8
DOI: https://doi.org/10.5753/sbc.4587.8

na vida das pessoas e como elas percebem e usam as tecnologias. A privacidade é um destes valores humanos, que no contexto da tecnologia, trata diretamente de informações ou dados de usuários.

Recentemente em 2018, a *General Data Protection Regulation* (GDPR) foi estabelecida na Europa, que regula no direito europeu a privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia e Espaço Econômico Europeu. Esta regulação veio como requisito para todas as organizações que tratam de dados de usuários em seus sistemas, e em caso de não conformidade, multas severas seriam aplicadas. No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), inspirada na GDPR, também regulamenta nacionalmente práticas de privacidade que impactam na atuação de organizações e na prática tecnológica (Brasil, 2018).

A privacidade se tornou então um requisito imprescindível no design das tecnologias em construção e das tecnologias existentes. Entretanto, essa consideração de privacidade pode ser apenas um desejo de não receber sanções ou multas, como uma situação de conformidade regulada por leis [Schaub et al., 2016]. Há diferença desse caso anterior com a privacidade ser considerada como um valor ou aspecto importante da proteção e do uso cotidiano de tecnologias pelas pessoas, sendo considerada como um valor pertencente à vida social das pessoas que implica em procedimentos formalizados de projeto e em escolhas técnicas de desenvolvimento.

Outra prática existente de projeto de privacidade, preocupada com conformidade legal, é modificar o sistema para seguir recomendações de privacidade quando o sistema já está em funcionamento, com usuários existentes, dados coletados, armazenados etc. A consideração de privacidade apenas quando o sistema já está pronto, após seu projeto e implementação, não tem beneficiado a construção de confiança e o conhecimento de privacidade pelos usuários. É relevante que projetistas considerem a privacidade como um valor a ser construído desde as primeiras etapas de concepção da tecnologia, evoluindo o entendimento do projeto e seus artefatos concretos juntamente com a privacidade, uma prática que pode ser apontada como "privacidade desde cedo" *ou "Early Privacy"* [Silva Junior et al., 2018b].

Neste propósito de *Early Privacy*, algumas práticas e metodologias já são existentes na literatura, como diretrizes para favorecer o estabelecimento da confiança e o respeito à privacidade dos usuários [Yamauchi et al., 2016], o método *Privacy by Design* [Langheinrich, 2001; Cavoukian, 2009], e um método para elicitação de requisitos de privacidade [Silva Junior et al., 2018a; Silva Junior et al., 2018b] e, por fim, o *Privacy Impact Assessment* (PIA) [Clarke, 1989; Clarke, 2009].

Este minicurso procura despertar os profissionais de TI para o *Early Privacy*, pensando a privacidade na fase inicial do projeto, abordando os métodos existentes e casos práticos de uso. A partir destes métodos e casos espera-se contribuir para a evolução do senso de design para um projetista ser capaz de produzir um processo concreto de design que seja consciente da privacidade, auxiliando a reduzir riscos de vigilância de dados, e construindo sistemas do futuro com preocupação de privacidade de diferentes grupos de usuários desde o início do projeto.

O trabalho está organizado da seguinte forma: a seção 2 introduz o conceito de privacidade, seus principais desafios na era da informação; a seção 3 apresenta alguns artefatos para o projeto de privacidade juntamente à uma visão crítica aos mesmos; a seção 4 aborda um

Minicursos da X Escola Regional de Informática de Mato Grosso
ISBN: 978-85-7669-487-8
DOI: https://doi.org/10.5753/sbc.4587.8

exemplo prático de uso destes artefatos para o projeto de privacidade, e, por fim, na seção 5, as considerações finais.

2. A Privacidade na era da Informação

As definições de privacidade datam desde 1890, quando advogados chamados Warren e Brandeis descreveram privacidade como "o direito de ser deixado em paz". Essa definição de privacidade se referia à proteção da vida pessoal de indivíduos, que poderia ser violada a partir de novos dispositivos de captura, como a câmera fotográfica [Langheinrich, 2018]. O corpo físico dos indivíduos e o espaço territorial pessoal eram os principais elementos de preocupação inicial dessa privacidade.

Com o advento dos sistemas computacionais, Westin (1968) definiu privacidade como a reivindicação de indivíduos, grupos ou instituições para determinar para si quando, como e em que medida as informações sobre eles são comunicadas para outros. Essa definição foi o início do que Westin chamou de "privacidade de informação": o direito de selecionar qual informação pessoal sobre mim é conhecida para quais pessoas. Esta definição está relacionada ao principal tipo de visão de privacidade digital, que é relacionada ao controle e coleta de dados [Dai et al., 2007].

Neste sentido, a pesquisa no campo de privacidade busca desenvolver a área de aviso e controle (ou *notice and control*, em inglês): a maneira como se informa sobre privacidade e apresenta os mecanismos necessários para sua configuração. Controle "significa dar aos consumidores opções sobre como qualquer informação pessoal coletada a partir deles podem ser usadas" [FTC, 1998]. Aviso diz respeito sobre os motivos sobre a coleta e uso da informação, entre outros [Commerce, 2000].

No mundo conectado por tecnologias digitais, com implementação concreta de produtos de Internet das Coisas (IoT), há um cenário de coleta e produção de dados de forma desenfreada, assim como a presença de câmeras, drones e outros dispositivos quase em todos os lugares da vida cotidiana, implicando em riscos para a privacidade nunca antes vistos. Nos contextos de IoT, o risco de privacidade se torna mais agudo pois todos os sensores combinados presentes em um ambiente podem prover informação detalhada sobre um usuário, por exemplo pode-se inferir maiores informações além das coletadas, como comportamento [Schaub et al., 2015].

Um exemplo do cenário complexo de privacidade e dispositivos tecnológicos é o de Hong Kong, em que dispositivos de reconhecimento facial estão sendo usados como forma de vigilância e estão sendo combatidos por parte da população que quer garantir sua anonimidade [New York Times, 2019]. Outro caso, envolvendo o Facebook e a empresa Cambridge Analytica, se comprovou a coleta indevida de dados de mais de 50 milhões de pessoas, com o objetivo de propaganda política na eleição presidencial dos Estados Unidos [New York Times, 2018].

Os assistentes pessoais, que coletam dados continuamente em contextos privados, também são exemplos de dispositivos que apresentam riscos para a privacidade. A Microsoft, após suspeitas sobre o tratamento dos dados coletados pela assistente pessoal Cortana, atualizou sua política de privacidade afirmando que empregados humanos podem escutar parte de suas interações diárias com a assistente Cortana para treinamento da inteligência artificial (métodos

ISBN: 978-85-7669-487-8
DOI: https://doi.org/10.5753/sbc.4587.8

manuais de processamento de áudio). Os áudios coletados poderiam possuir informações sensíveis, como dados de cartão, discussões, entre outros [The Verge, 2019].

Estes cenários apenas indicam a relevância de um problema atual que pode provocar maiores riscos à vida de usuários. Alguns riscos de privacidade já foram apontados na literatura, como o compartilhamento de dados pessoais com terceiros sem consentimento [Silva Junior et al., 2018b], a vigilância em massa, a não verificação ou compreensão da coleta de dados por usuários [Ponciano et al., 2017] e o próprio comportamento descuidado do usuário quer seja por falta de conhecimento, dificuldade no acesso à informação ou por livre escolha, o que nos remete ao Paradoxo da Privacidade [Kokolakis, 2017].

Estes casos de violações de privacidade motivaram o cenário de privacidade voltar sua atenção para normas e regulamentos, atuando de forma regulatória a nível governamental. A GDPR (*General Data Protection Regulation*) é um regulamento criado em 2016 com o propósito de regular a coleta, tratamento e compartilhamento de dados pessoais de cidadãos e residentes da União Europeia, dando maior controle aos indivíduos sobre informações pessoais coletadas. Em 2018 o regulamento entrou em vigor, implicando em mudanças nas empresas de tecnologia que precisaram se adequar aos novos requisitos de privacidade.

No Brasil, inspirada na GDPR, a LGPD (Lei Geral de Proteção de Dados Pessoais) tem como objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural [Brasil, 2018]. A LGPD trata, dentre outros, do consentimento de usuários, de requisitos para tratamento de dados pessoais, e dos direitos para o usuário, como acesso, correção e eliminação dos dados coletados.

Deste modo, a privacidade digital está sendo formalizada de forma definitiva como um requisito legal que as tecnologias devem considerar. Instituída em legislações (GDPR, LGPD) com direitos e deveres definidos, o desafio agora é projetar a privacidade nos sistemas. Os novos sistemas a serem desenvolvidos devem pensar a privacidade desde o início de seu projeto, avançando o projeto e a construção da solução juntamente com requisitos de privacidade. É importante lembrar que as leis só podem trabalhar em conjunto com a realidade social e tecnológica, não contra elas [Langheinrich, 2011].

Entretanto, não há uma solução única e universal para dizer que uma solução é segura para a privacidade: é preciso considerar cada sistema, o que o sistema faz, quais são as implicações disso, e depois descobrindo como (e por quê) isso precisa ser alterado para alcançar o comportamento correto [Langheinrich, 2018]. Desenvolver um sistema apenas para cumprir com o que a lei demanda fará com que um sistema tenha a privacidade voltada para dispositivos legais, não com o intuito explícito de auxiliar e proteger usuários.

Na próxima seção são apresentados artefatos de projeto de privacidade, que auxiliam projetistas de software a lidar com a complexidade da privacidade. Os artefatos também buscam trazer uma visão de projeto de privacidade que seja mais centrada no usuário, ajudando-o a fazer decisões acertadas, ter liberdade em sua escolha e poder sobre seus dados.

3. Métodos de Projeto de Privacidade

Nesta seção são apresentados os artefatos que projetistas podem utilizar para pensar a privacidade em seus sistemas. Os artefatos são principalmente diretrizes e princípios, que dizem

Minicursos da X Escola Regional de Informática de Mato Grosso
ISBN: 978-85-7669-487-8
DOI: https://doi.org/10.5753/sbc.4587.8

como fazer algo e pontos importantes de análise; um método para elicitar requisitos de privacidade a partir de uma sequência de passos que pode envolver usuários da tecnologia que se quer projetar e, também um processo para analisar e minimizar possíveis impactos e implicações da perda de privacidade.

3.1 *Privacy by Design* e Diretrizes de Privacidade

Privacy by Design (PbD) é a incorporação da privacidade no design de tecnologias nos estágios iniciais do processo de desenvolvimento e durante todo o ciclo de vida de seu desenvolvimento [Hadar et al., 2017]. PbD é indicada por meio de um conjunto de seis princípios para orientar o projeto do sistema, sendo [Langheinrich, 2001]:

1. Aviso: nenhuma coleta de dados pode passar despercebida ao sujeito que está sendo monitorado (desde que o indivíduo possa ser identificado pessoalmente). Dependendo do tipo de dispositivo, diferentes mecanismos de *notice* precisariam ser encontrados. O objetivo é enumerar exaustivamente todos os tipos de dados coletados, não os dispositivos individuais que o fazem. Não importa quantos sensores gravam dados de áudio em uma determinada sala - o fato de ocorrer uma gravação de áudio que é a informação importante.
2. Escolha e Consentimento: não basta mais anunciar e declarar a coleta de dados - também é necessário que os "coletores" recebam consentimento explícito do titular dos dados. Não basta mais anunciar e declarar a coleta de dados - também exige que os coletores recebam o consentimento explícito do titular dos dados. Outro problema relacionado à noção de consentimento é o requisito de escolha: com apenas uma opção disponível, obter consentimento pode ser considerado chantagem. Para tornar o consentimento uma opção viável, é necessário oferecer mais do que o dualismo de "pegar ou largar".
3. Anonimato e Pseudonimato: O anonimato pode ser definido como "o estado de não ser identificável em um conjunto de assuntos". Uma opção importante ao oferecer aos clientes diversas opções, para que aqueles que desejam permanecer anônimos possam permanecer assim. Seja anônimo ou pseudônimo - se os dados não puderem ser rastreados até um indivíduo (ou seja, se for impossível de ser ligado), a coleta e o uso desses dados não representam uma ameaça à privacidade dos indivíduos.
4. Proximidade e Localidade: dispositivos pessoais (como roupas "inteligentes") possam gravar conversas e comportamentos sempre que o proprietário estiver presente. No caso de o proprietário deixar acidentalmente esse dispositivo para poder testemunhar uma conversa ou reunião de outras pessoas em sua ausência, todo o equipamento sensorial será desligado até que a presença do proprietário seja detectada novamente. Na noção de localidade, as informações podem simplesmente estar ligadas aos locais em que são coletadas. Há uma exigência de que a informação não fosse disseminada indefinidamente, mesmo que não fosse por meio de um limite geográfico maior, como prédios ou salas. As informações coletadas em um edifício permaneceriam na rede do edifício.
5. Segurança Adequada: autenticidade e comunicações confiáveis. Dispositivos ubíquos introduzirão todo um novo conjunto de restrições, principalmente nas áreas de consumo de energia e protocolos de comunicação. Grande parte dessa complexidade pode ser

Minicursos da X Escola Regional de Informática de Mato Grosso
ISBN: 978-85-7669-487-8
DOI: https://doi.org/10.5753/sbc.4587.8

reduzida, empregando segurança robusta apenas em situações com transferência de dados altamente sensível.

6. Acesso e Recurso: Confiar em um sistema requer um conjunto de regulamentos que separem comportamentos aceitáveis de inaceitáveis, juntamente com um mecanismo razoável para detectar violações e aplicar as penalidades estabelecidas nas regras. A tecnologia pode ajudar a implementar requisitos legais específicos, como limitação de uso, acesso ou repúdio.

PbD não tenta alcançar nem segurança nem privacidade total de soluções tecnológicas, pois reconhece que a vigilância e ações mal intencionadas podem ocorrer [Langheinrich, 2001]. Deste modo, PbD é uma opção para que a privacidade seja de fato considerada no projeto de tecnologias. Cavoukian (2009) acrescenta mais 7 princípios de PbD, sendo estes:

1. Proativo não reativo; preventivo, não corretivo: antecipa e evita eventos invasivos de privacidade antes que eles aconteçam. O PbD não espera que os riscos de privacidade se materializem, nem oferece remédios para resolver infrações de privacidade depois que elas ocorrerem - ele visa impedir que elas ocorram. Em resumo, PbD vem antes do fato, não depois.
2. Privacidade como padrão: busca oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de Tecnologia de Informação (TI) ou prática comercial. Se um indivíduo não faz nada, sua privacidade ainda permanece intacta. Nenhuma ação é necessária por parte do indivíduo para proteger sua privacidade - ela é incorporada ao sistema, por padrão.
3. Privacidade incorporada ao design: a privacidade não é estendida como um complemento, após o fato. A privacidade é um componente essencial da funcionalidade principal que está sendo entregue. A privacidade é parte integrante do sistema, sem diminuir a funcionalidade.
4. Funcionalidade total - soma positiva, não soma zero: procura acomodar todos os interesses e objetivos legítimos de maneira positiva, com “ganhos em dobro”, e não através de uma abordagem datada de soma zero, onde são feitas compensações desnecessárias. O PbD evita a pretensão de falsas dicotomias, como “privacidade *versus* segurança”, demonstrando que é possível e muito mais desejável ter as duas.
5. Segurança de ponta a ponta - proteção do ciclo de vida: tendo sido incorporado ao sistema antes do primeiro elemento de informação ser coletado, estende-se com segurança por todo o ciclo de vida dos dados envolvidos — fortes medidas de segurança são essenciais para a privacidade, do início ao fim. Isso garante que todos os dados sejam retidos com segurança e destruídos com segurança no final do processo, em tempo hábil. Assim, o PbD garante do começo ao fim o gerenciamento seguro e seguro das informações, de ponta a ponta.
6. Visibilidade e Transparência: procura garantir a todas as partes interessadas que, independentemente da prática ou tecnologia de negócios envolvida, esteja de fato operando de acordo com as promessas e objetivos declarados, sujeita a verificação independente. Seus componentes e operações permanecem visíveis e transparentes, tanto para usuários quanto para fornecedores.

Minicursos da X Escola Regional de Informática de Mato Grosso
ISBN: 978-85-7669-487-8
DOI: https://doi.org/10.5753/sbc.4587.8

7. Respeito pela privacidade do usuário: exige que arquitetos e operadores mantenham os interesses do indivíduo em primeiro plano, oferecendo medidas como padrões de privacidade fortes, aviso apropriado e opções poderosas para o usuário. Mantenha centrado no usuário.

Com preocupações diferentes das apresentadas nestes princípios, Yamauchi et al. (2016) apresentam 10 diretrizes para o estabelecimento de privacidade em sistemas ubíquos. A seguir, as 10 diretrizes são apresentadas em sua íntegra.

1. Usar linguagem clara: a aplicação deve possuir uma linguagem clara e simplificada para expressar as consequências de privacidade e das escolhas dos usuários, de modo que o usuário veja o impacto de suas decisões sem ler muito, ao tempo em que a mensagem não seja curta demais a ponto de deixar passar informações relevantes.

2. Permitir checagem e liberdade de configuração: a aplicação deve possibilitar ao usuário a checagem, de forma fácil, de suas configurações de privacidade ao tempo em que deve dar liberdade ao usuário para alterar estas configurações.

3. Possuir clara finalidade de uso de dados: uma aplicação deve sempre informar ao usuário para quais fins as suas informações pessoais serão utilizadas.

4. Realizar coleta mínima de dados: uma aplicação deve coletar somente os dados necessários para prover seus serviços ao usuário, evitando assim coleta de dados desnecessária e garantindo a privacidade do usuário.

5. Permitir controle e transparência de dados: o usuário deve ter controle de como seus dados estão sendo armazenados e compartilhados, e ter conhecimento do tempo de latência máximo que os dados poderiam ficar armazenados após a exclusão da conta. Com exceção de casos em que as informações fizerem parte de ações judiciais, o usuário poderia ser notificado quando os dados foram definitivamente excluídos do servidor.

6. Utilizar mecanismos de segurança: uma aplicação deve ter os dados pessoais de seus usuários protegidos utilizando medidas de segurança como criptografia, testes de vulnerabilidades, entre outros, a fim de garantir a integridade dos dados de seus usuários de ataques de terceiros ou vulnerabilidades dos sistemas e ampliar a confidencialidade do usuário sobre informações compartilham.

7. Obedecer a legislação vigente: uma aplicação deveria atender a legislação vigente do país em que está em uso e não somente a legislação do país em que foi criada.

8. Flexibilizar os termos de uso e políticas de privacidade: os termos deveriam prover certa flexibilidade ao acesso aos recursos do smartphone e ser projetados de forma mais interativa. Por exemplo, há aplicações que utilizam diversas ferramentas do smartphone como microfone, GPS, acesso à lista de contatos; se o usuário optar por não querer que a aplicação acesse a lista de contatos a aplicação deve fornecer algum tipo de flexibilidade para a escolha do usuário, em especial quando este tipo de acesso não é crucial para a funcionalidade ao qual o aplicativo se propõe.

9. Notificar o usuário quando houver alteração em algum termo: o usuário deve ser informado de maneira clara quando há mudança em qualquer termo do aplicativo. Por exemplo, ao iniciar o aplicativo, o usuário deveria ser notificado de qualquer alteração no termo de uso e/ou na política de privacidade, demonstrando de forma clara uma comparação entre as versões “velha” e “nova” do texto.

Minicursos da X Escola Regional de Informática de Mato Grosso
ISBN: 978-85-7669-487-8
DOI: https://doi.org/10.5753/sbc.4587.8

10. Disponibilizar os termos no idioma do aplicativo: os termos de uso e as políticas de privacidade deveriam estar escritos no idioma em que está o aplicativo, sob o ponto de vista que os termos são parte do aplicativo e como tal, precisam promover clareza e melhor entendimento dos usuários.

As diretrizes adicionam aspectos novos para o design de tecnologias, como ter os termos de privacidade na língua do país em que o dispositivo opera, obedecer a legislação vigente, clara finalidade de uso de dados e coleta mínima de dados. Juntamente com os princípios de PbD formam um conjunto robusto de elementos que são importantes para o estabelecimento de privacidade e que podem ser conhecidos por projetistas e desenvolvedores desde o início do projeto, como "regras de ouro" a serem seguidas.

Enquanto estes princípios são elementos abrangentes de análise para o design de privacidade, eles ainda estão longe de serem utilizados de forma difundida no mercado, com poucos exemplos de implementação bem sucedida de PbD [Hadar et al., 2017]. Um dos motivos pode ser o esforço adicional de pensar sobre a privacidade nos sistemas; e a contradição da privacidade com modelos de negócios baseados na coleta de dados e vigilância. Entretanto, as próprias abordagens de projetar e implementar privacidade ainda possuem pontos fracos e lacunas, por exemplo, os princípios de PbD são considerados vagos [Hadar et al., 2017].

As preferências de usuários sobre sua privacidade também podem não estar sendo refletidas nos sistemas desenvolvidos [Hadar et al., 2017], o que sugere um distanciamento entre o que o usuário deseja e o que é de fato desenvolvido no sistema. Esse distanciamento tem como uma das possíveis causas o distanciamento entre o modelo mental do usuário e desenvolvedor sobre as tecnologias. Modelos mentais são representações de como algo funciona ou deve funcionar. O distanciamento entre modelo mentais de usuário e desenvolvedor pode ocorrer devido também ao fato de que usuários podem não possuir um modelo mental (não possuir um entendimento) sobre novas tecnologias que não utilizou antes, pois os modelos mentais são desenvolvidos a partir de experiências passadas [Lowdermilk, 2013].

Este distanciamento de modelos mentais é um desafio que motivou a construção do Método de Elicitação de Requisitos de Privacidade, envolvido no conceito de *Early Privacy* [Silva Junior et al., 2018b], que apresentamos na próxima seção juntamente com a técnica *Privacy Impact Assessment* (PIA) [Clarke, 1989, Clarke, 2009].

3.2 *Early Privacy*, Método de Elicitação de Requisitos de Privacidade e *Privacy Impact Assessment*

Em *Early Privacy,* a privacidade não é pensada apenas como um requisito legal e técnico, mas como um valor a ser levado em todas as fases de projeto e desenvolvimento, contribuindo para que a privacidade seja então reconhecida como um direito fundamental humano. A concepção de *Early Privacy* não envolve somente a privacidade, mas também a acessibilidade ou design universal, garantindo que a privacidade seja acessada, entendida e usada na maior medida e pela maior quantidade de pessoas possível. E por fim, *Early Privacy* envolve a usabilidade, construindo instrumentos de acesso, compreensão e ação sobre a privacidade que possibilitem a fácil utilização por seus usuários.

Minicursos da X Escola Regional de Informática de Mato Grosso
ISBN: 978-85-7669-487-8
DOI: https://doi.org/10.5753/sbc.4587.8

A *Early Privacy* tem seu conceito apoiado por um Método de Elicitação de Requisitos de Privacidade [Silva Junior et al, 2018a]. Como requisitos são elementos formais levantados nas fases iniciais de projeto de um sistema, um método que auxilia a levantar requisitos de privacidade de forma centrada no usuário auxilia então a privacidade ser formalizada desde cedo no projeto de uma tecnologia. Este método é composto das seguintes etapas [Silva Junior et al, 2018a]:

1. Desenvolvimento e Aplicação de Questionário: usuários possuem diferentes comportamentos em relação à privacidade. Deve-se pensar nos diversos grupos que podem ser afetados pelo software, destacando suas necessidades e comportamentos, que podem ser levantados por meio de questionários. O questionário deve procurar abordar o contexto em que o sistema atuará e questões sobre práticas de privacidade do respondente, como preocupações e expectativas.
2. Desenvolvimento de Personas: a partir de alguns comportamentos de privacidade relacionados ao sistema que se quer produzir, levantados pelo questionário, pode-se pensar representações deste grupo por meio de personas, onde projetistas pensam o software a partir de indivíduos "reais", para assim poder "apreciar melhor se o design foi ou não bem-sucedido em satisfazer a persona".
3. Desenvolvimento de cenários: após a representação da extensão dos grupos de usuários, projetistas podem materializar seus modelos mentais por meio da técnica de cenários, que possui capacidade de elicitar requisitos de sistema ainda não concebidos, descrevendo histórias que podem abordar diferentes aspectos do sistema, problemas e perspectivas de projeto, além de auxiliar na investigação de situações futuras.
4. Seleção de Usuários: deve-se selecionar usuários que pertençam ao perfil determinado para participar da aplicação do método, pois só assim se verifica em um contexto real seu modelo mental, expectativas, desejos e particularidades de privacidade.
5. Apresentação e Discussão do Cenário: o projetista deve apresentar o cenário para os usuários e, a partir da discussão do cenário, identificar desejos, expectativas ou inquietações. Projetistas e Usuários podem questionar pontos específicos do cenário entre si, como o que marcou negativamente no cenário ou aspectos que gostariam que fossem diferentes.
6. Re-design do Cenário e Construção de Protótipos: após a formação inicial do modelo mental do usuário sobre o sistema em discussão, o projetista deve entender este modelo mental, a partir da reescrita do cenário pelo usuário e braindrawing (prototipação colaborativa livre) de interfaces para a construção de protótipos de baixa fidelidade.
7. Aplicação de Questionário pós-sessão: após a discussão entre usuários e projetista, pode-se elicitar maiores pontos a partir de questionários e entrevistas pós-sessão, avaliando com perguntas específicas a transformação de pensamento do usuário em relação à privacidade, quais práticas de dados são vistas como mais pretendidas e suas preocupações em relação a elas.

O método pode ser associado ainda com os princípios de PbD, por exemplo utilizando no cenário ações relacionadas a um ou mais princípios, ou perguntando diretamente a usuários sobre sua opinião em relação a uma ou mais prática descrita em um princípio.

ISBN: 978-85-7669-487-8
DOI: https://doi.org/10.5753/sbc.4587.8

O método busca envolver usuários a fim de compreender seu modelo mental da tecnologia e aproximá-lo do modelo mental de projetistas e, apesar de ser uma opção viável para o projeto de privacidade, o método tem um esforço adicional por envolver usuários. Esse esforço adiciona maior custo de tempo e recursos (financeiro, pessoal) no desenvolvimento de uma solução. Acredita-se que desenvolver uma aplicação que respeite a privacidade de seus usuários pode contribuir para manter um público que confia na tecnologia que usa, fazendo com que o esforço adicional valha a pena.

Por fim, *Privacy Impact Assessment* (PIA) é uma técnica que vem evoluindo desde os meados de 1990, utilizada em vários países como Canadá, Austrália, Nova Zelândia e Reino Unido [Clarke, 2009]. PIA possui várias definições, como a de Clarke (1989): um processo pelo qual os possíveis impactos e implicações de propostas que envolvem potencial invasão de privacidade são analisados e examinados; ou a de Wright (2012): metodologia para avaliar os impactos na privacidade e, em consulta com as partes interessadas, tomar ações corretivas a fim de evitar ou minimizar impactos negativos.

De modo geral, quando se trata de Tecnologia de Informação, PIA é um processo para identificar riscos e impactos para a privacidade de usuários que algum sistema computacional implica quando é projetado, implementado e utilizado, assim como tomar medidas para mitigar estes riscos e impactos. Por isso uma PIA deve começar nos estágios mais iniciais possíveis, quando ainda existem oportunidades para influenciar o resultado de um projeto [Wright, 2012], por exemplo ao mudar a forma de armazenar os dados coletados.

De acordo com Clarke (2009), PIA tem as características de ser realizada em um projeto ou iniciativa, com natureza antecipatória; possui amplo escopo em relação às dimensões da privacidade, permitindo considerar a privacidade da pessoa, de seus dados, comportamento e comunicação; é orientada tanto para problemas quanto soluções; enfatiza o processo de avaliação, incluindo troca de informações, aprendizado organizacional e adaptação do projeto; e requer envolvimento intelectual de executivos e gerentes seniores.

Há várias formas de se executar uma PIA, variando por exemplo por país (Austrália, Reino Unido, Estados Unidos). Com 14 passos, Wright (2013) apresenta uma metodologia otimizada, ou mais robusta para se realizar uma PIA. De modo geral, a seguir são apresentados passos mais concisos para execução de uma PIA [OAIC, 2014]:

1. Avaliação sobre necessidade da PIA: determina a necessidade de realizar uma PIA completa ou não. Se algum tipo de dado pessoal for coletado, armazenado, usado ou compartilhado, provavelmente o projeto pode se beneficiar de uma PIA.
2. Planejamento: bom planejamento garantirá uma PIA eficaz e eficiente.
3. Descrever: fornece contexto para o projeto para que todas as partes interessadas envolvidas entendam.
4. Identifique e consulte as partes interessadas: quem está interessado ou é afetado pelo projeto?
5. Mapear fluxos de informações: quais informações serão coletadas, usadas e divulgadas, como serão mantidas e protegidas e quem terá acesso a elas?
6. Análise de impacto de privacidade e verificação de conformidade: como o projeto afeta a privacidade e é compatível com Princípios de Privacidade?

ISBN: 978-85-7669-487-8
DOI: https://doi.org/10.5753/sbc.4587.8

7. Gerenciamento de privacidade - abordando riscos: que opções você tem para remover, minimizar ou mitigar qualquer impacto negativo na privacidade?
8. Recomendações: faça recomendações sobre como os riscos evitáveis podem ser removidos ou reduzidos para um nível mais aceitável.
9. Relatório: resume suas descobertas e recomendações.
10. Responder e revisar: implementação de recomendações e monitoramento contínuo.

A PIA é considerada um processo maduro, com várias aplicações em órgãos governamentais e com exemplos de relatórios de PIA disponibilizadas de forma transparente. Entretanto, pode ser custosa para realizar em uma grande organização (ou sistema), pode depender do envolvimento de vários membros de uma equipe para que seja finalizada e necessitar de apoio de pessoal técnico para identificar riscos de privacidade e suas respectivas soluções.

4. Projetando a Privacidade em um Cenário Fictício

Nesta seção, é apresentado um exemplo de uso dos artefatos que foram apresentados nas Seção 3 a partir de um cenário fictício de uma solução de IoT para um ambiente domiciliar.

Imaginemos que uma solução de IoT busca coletar dados de consumo de água e de energia dentro de uma casa. A partir destes dados a solução produz relatórios de consumo e indica pontos de maior gasto e possíveis condições de economia. Essa solução pode coletar, armazenar e processar muitos dados sensíveis, o que implica na relevância de ser um projeto que considere a privacidade de seus usuários (membros do domicílio).

Como um provável projetista ou membro da equipe de desenvolvimento, poderíamos utilizar o Método de Elicitação de Requisitos de Privacidade e as diretrizes para auxiliar no projeto desta solução pensando em privacidade. No Método, o primeiro passo é a construção de um questionário para verificar os diversos grupos a serem afetados pelo software. Neste caso, o propósito é então identificar os *stakeholders* que possivelmente serão impactados pela solução, os membros do domicílio ou de uma família. Estes *stakeholders* podem ser divididos de várias formas, neste caso uma divisão poderia ser em moradores adultos (pais, avós, tios etc.), jovens (filhos mais velhos, etc.), crianças (filhos mais novos etc.) e possíveis vizinhos da casa (adultos, jovens e crianças). Cada um destes grupos de *stakeholders* podem produzir dados diferentes de consumo na casa e serem afetados de forma diferente por uma solução.

O segundo passo do método é o desenvolvimento de personas (*para exemplos de métodos e formulários para a criação de personas, veja* [Ferreira et al 2018]). O propósito de utilizar personas é tornar concreto para a equipe de desenvolvimento os grupos de possíveis usuários da solução. Neste caso, utilizaremos uma persona já desenvolvida, chamada Júlia, que representa uma usuária jovem, usuária de aplicativos móveis e de redes sociais, em que faz postagens diariamente com algum conhecimento e manipulação de configurações de privacidade [Cerqueira, 2013]. Com essas informações de uma provável usuária, tem-se um contexto para investigar como a privacidade de dados pode ocorrer. Para isso, os princípios de PbD e algumas questões dentro de uma PIA podem ser utilizadas, por exemplo:

- PIA - Qual informação pessoal será coletada, armazenada, usada ou divulgada como parte do seu projeto?

ISBN: 978-85-7669-487-8
DOI: https://doi.org/10.5753/sbc.4587.8

    - consumo de água e energia de chuveiro, com registro de horário, duração de banho, picos de uso de energia e histórico ao longo do tempo de uso do chuveiro em cada banheiro da casa.
    - consumo de energia (luz, tomadas) em cada cômodo da casa, com registro de horário, duração e intensidade.
- PbD - Princípio Visibilidade e Transparência: como deixar as informações de coleta de dados de fácil entendimento para Júlia? Como dar visibilidade quando algum tipo de coleta estiver ocorrendo? Como evitar que a coleta pareça com algum tipo de vigilância?

Essas investigações exploratórias podem ser feitas de modo profundo pela equipe de desenvolvimento, a partir de um subconjunto maior de perguntas da PIA ou de princípios de PbD ou de estabelecimento de privacidade. A partir destas investigações a equipe pode então selecionar os pontos mais importantes para explorar no próximo passo (terceira etapa) do método, desenvolvimento de cenários.

Cenário é uma história ou narrativa que descreve um personagem e suas ações em um ambiente específico com o propósito de ilustrar contextos de problemáticas existentes e utilização de uma solução. Neste caso, utilizaremos também um cenário já desenvolvido [Silva Junior et al., 2018a], no qual esta solução de monitoramento domiciliar é descrita. No cenário, uma usuária chamada Marta vive com os pais, utiliza apps e lida com problemas quando um sistema inteligente de economia de energia e água é instalado em sua casa, em que seu pai começa a perceber seu comportamento de consumo dentro de casa e Marta não consegue saber exatamente como o sistema funciona ou como os dados são coletados.

Neste cenário, são exploradas especificamente problemáticas relacionadas ao princípio de Aviso do Pbd, pois Marta não tem ciência que os dados tinham sido coletados; e às diretrizes de “Flexibilizar os termos de uso e políticas de privacidade” e “Possuir clara finalidade de uso de dados”, pois Marta não consegue compreender como os dados são coletados, como o sistema funcionava e não tinha opção de desativar a coleta em alguns momentos específicos. Em outro projeto, o cenário poderia refletir diversas outras problemáticas que seriam utilizadas para levantar discussões com usuários (quarta etapa do Método- seleção de usuário; quinta etapa - apresentação e discussão do cenário) se algo deveria ser e como deveria ser implementado. Com essa discussão, usuários poderiam deixar claro para desenvolvedores quais práticas concordam, esperam e quais suas expectativas para a possível solução descrita no cenário.

Após essa discussão, a sexta etapa do método é o redesign do cenário e construção de protótipos, adentrando em uma natureza mais prática com usuários selecionados, em que o projetista pode entender o modelo mental de quem irá utilizar a solução.

Por fim, a última etapa do método consiste em aplicação de um questionário pós-sessão com usuários. Neste questionário, algumas questões específicas da PIA poderiam ser utilizadas para verificar a compreensão de usuários sobre alguns riscos. Por exemplo [OIAC, 2014]:

- Como usuários preferem ter controle sobre sua informação?
- Os impactos de privacidade (e.g., vigilância) são justificados em proporção ao benefício que a solução oferece?
- O uso de informações pessoais em seu projeto está alinhado com as expectativas da comunidade?

ISBN: 978-85-7669-487-8
DOI: https://doi.org/10.5753/sbc.4587.8

Em cada uma destas etapas, a equipe pode identificar requisitos de projeto, restrições para a proposta de solução e oportunidades para construção de novas funcionalidades. A equipe também pode identificar como cada princípio ou diretriz de privacidade se tornou um requisito ou característica de seu projeto, verificando quais princípios ou diretrizes não implicaram em nenhum elemento de privacidade para o projeto. Estes princípios ou diretrizes poderiam ser explorados para que surgissem requisitos novos para o projeto, caso aplicável.

5. Considerações Finais

Este capítulo tratou de conceitos e temas relevantes para o estabelecimento da privacidade desde o princípio, junto com o entendimento do contexto da solução e do projeto de um sistema. Foram apresentados princípios, diretrizes, um método e um processo que formam um arsenal inicial de possibilidades para apoiar projetistas a entenderem a privacidade e defini-la em seus projetos.

Avanços no campo legislativo indicam um cenário de maior preocupação com a privacidade. Entretanto, também é possível observar as constantes violações aos direitos de privacidade de indivíduos. Deste modo, enquanto se tem uma visão positiva sobre o futuro da privacidade, ao mesmo tempo há um desafio a ser superado sobre a tensão entre privacidade, desejos comerciais, tecnológicos ou governamentais e os riscos implicados pela capacidade computacional dos dispositivos, seja de coleta, processamento ou inferência de informações.

Projetar a privacidade ainda é um desafio da Computação e suas áreas, como Interação Humano-Computador e Engenharia de Software. Os artefatos apresentados são contribuições importantes para a privacidade de informação, mas ainda devem evoluir para apoiar de forma mais efetiva e concreta a evolução da privacidade nos sistemas e para auxiliar projetistas de forma cada vez mais explícita e sistematizada para o projeto de privacidade.

Referências

Brasil. (2018) “Lei Nº 13.709”. Acesso em: 05/10/2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> .

Cavoukian, A. (2009) “Privacy by design: The 7 foundational principles.” Information and Privacy Commissioner of Ontario, Canada 5.

Clarke, R. (1989) “Privacy Impact Assessment Guidelines”. Acesso em: 05/10/2019. Disponível em: <http://www.xamax.com.au/DV/PIA.html>

Clarke, R. (2009) “Privacy impact assessment: Its origins and development”. Computer Law & Security Review, 25(2), 123–135. doi:10.1016/j.clsr.2009.02.002

Cerqueira, T. R. (2013) “Personas como Método de Avaliação – Um Estudo Sobre a Usabilidade das Configurações de Privacidade do Facebook”. Monografia Especialização. UFMT.

Kokolakis, S. (2017) “Privacy Attitudes and Privacy Behaviour: a review of current research of the privacy paradox phenomenon”, In: Computers and Security, v. 64, 2017, p. 122-134.

ISBN: 978-85-7669-487-8
DOI: https://doi.org/10.5753/sbc.4587.8

Langheinrich M. (2001) “Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems”. In: Abowd G.D., Brumitt B., Shafer S. (eds) Ubicomp 2001: Ubiquitous Computing. UbiComp 2001. Lecture Notes in Computer Science, vol 2201. Springer, Berlin, Heidelberg

Lowdermilk, T. “User-centered design: a developer’s guide to building user-friendly applications”. O’Reilly Media, Inc, 2013.

Langheinrich, M. (2018) "Privacy in Ubiquitous Computing." Ubiquitous computing fundamentals. Chapman and Hall/CRC, 109-174.

New York Times. (2019) “In Hong Kong Protests, Faces Become Weapons”. Acesso em: 16/09/2019. Disponível em: https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html

New York Times. (2018) “Cambridge Analytica and Facebook: The Scandal and the Fallout So Far”. Acesso em: 16/09/2019. Disponível em: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

Ponciano, L., Barbosa, P., Brasileiro, F., Brito, A., & Andrade, N. (2017) “Designing for Pragmatists and Fundamentalists: Privacy Concerns and Attitudes on the Internet of Things”. In Proceedings of the XVI Brazilian Symposium on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, Article 21, 1–10.

OAIC (Office of the Australian Information Commissioner). (2014) “Guide to undertaking privacy impact assessments”. Disponível em: <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/>

Sellen, A. Rogers, Y. Harper, R., and Rodden, T. (2009) “Reflecting human values in the digital age”. Commun. ACM 52, 3 (March 2009), 58-66.

Schaub, F., Breaux, T. D., and Sadeh, N. (2016) “Crowdsourcing privacy policy analysis: Potential, challenges and best practices.” it-Information Technology 58.5: 229-236.

Silva Junior, D. P., de Souza, P. C. and Maciel, C. (2018a) “Method for privacy requirements elicitation in ubiquitous computing”. In: Proceedings of the XXXII Brazilian Symposium on Software Engineering (SBES '18). ACM, New York, NY, USA, 178-183

Silva Junior, D. P., de Souza, P. C. and Gonçalves, T. A. J. (2018b) “Early Privacy: Approximating Mental Models in the Definition of Privacy Requirements in Systems Design.” In: Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems. ACM.

The Verge. (2019) “Microsoft’s new privacy policy admits humans are listening to some Skype and Cortana recordings”. Acesso em: 05/10/2019. Disponível em: <https://www.theverge.com/2019/8/14/20805801/microsoft-privacy-policy-change-humans-listen-skype-cortana-voice-recording>

Yamauchi, E. A., de Souza, P. C. and Silva Junior, D. P.. (2016) “Prominent issues for privacy establishment in privacy policies of mobile apps.” In: Proceedings of the 15th Brazilian Symposium on Human Factors in Computing Systems. ACM.

ISBN: 978-85-7669-487-8
DOI: https://doi.org/10.5753/sbc.4587.8

Wright, D. (2012) "The state of the art in privacy impact assessment." Computer Law & Security Review 28.1 (2012): 54-61.

Wright, D. (2013) “Making Privacy Impact Assessment More Effective”, The Information Society, 29:5, 307-315