Fall 10-16-2021

Analysis of the General Data Protection Regulation: Approach through Activity Theory

António Gonçalves
INESC-ID, agoncalveslx@gmail.com

Anacleto Correia
Escola Naval/CINAV, anacleto.correia@gmail.com

Análise do regulamento Geral de proteção de dados: Abordagem através da Teoria da atividade

Analysis of the General Data Protection Regulation: Approach through Activity Theory

António Gonçalves, IPS, INESC-ID, Portugal, agoncalveslx@gmail.com

Anacleto Correia, Escola Naval/CINAV, Portugal, anacleto.correia@gmail.com

Resumo

A segurança do tratamento dos dados pessoais consiste em garantir que as pessoas podem confiar numa organização para utilizar os seus dados de forma justa e responsável. Se uma entidade, no contexto do Espaço Europeu, realizar qualquer operação (i.e., tratamento) que utilize informações sobre pessoas por qualquer razão terá que cumprir com o Regulamento Geral de Proteção de Dados. Contudo, devido à sua complexidade, as abordagens tradicionais, de segurança da informação não reduzem o risco da proteção do tratamento de forma eficaz. Este artigo argumenta que temos de reconsiderar a nossa abordagem se quisermos lidar eficazmente com o problema do risco. Para tal é utilizada uma abordagem baseada no conceito de atividade presente na Teoria da Atividade. Esta teoria possui os componentes necessários para alcançar um objetivo comum dentro de um contexto, neste caso da proteção do tratamento dos dados pessoais.

Palavras-chave: segurança de informação; proteção de dados; dados pessoais; proteção do tratamento.

Abstract

Security of personal data processing is about individuals being able to trust that an organisation will handle their data fairly and responsibly. In the context of the European area, if an organisation carries out an operation (i.e. processing) involving information about individuals for any reason, it must comply with the General Data Protection Regulation. However, due to their complexity, traditional, information technology security approaches do not effectively reduce the security risk of the processing. This paper argues that we need to rethink our approach if we want to effectively address the problem of risk, and proposes an approach based on the concept of activity within activity theory, which has the necessary components to achieve a common goal within a context, in this case protection.

Keywords: *information security; data protection; personal data; protection of processing.*

1. INTRODUÇÃO

Os serviços são omnipresentes, mas não existe um padrão adequado para os descrever com precisão e não existe, tal como um produto num supermercado, um rotulo com um resumo ao qual está anexado para a segurança e benefício do consumidor. Podemos, contudo, definir a natureza de um serviço como um pacto, em que uma entidade (i.e., organização ou pessoa) faz algo por outra e que gera benefícios para ambas. (Edmond, OSullivan, & Hofstede, 2002).

Uma vez que os serviços fazem uso de dados que podem ser associados a uma pessoa, as entidades que prestam os serviços devem utilizar os dados pessoais segundo um conjunto de critérios. O Regulamento Geral de Proteção de Dados (RGPD) é o enquadramento, em vigor no Espaço Europeu, que as entidades têm que cumprir em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais de modo a assegurar os seus direitos à proteção dos dados pessoais e criar confiança no serviço. (Dibble, 2020).

A verificação da utilização adequada dos princípios do RGPD num serviço é relevante porque se não estiver alinhado com o RGPD pode levar ao fracasso do mesmo devido, por exemplo, à falta de qualidade, no que diz ao tratamento dos dados e acontecer uma violação de dados pessoais (Macaulay, 2012) .

Uma iniciativa da Comissão Europeia (CE) para recolher a opinião dos cidadãos europeus sobre a sua atitude relativamente à proteção de dados revelou que 69% estão preocupados com a possibilidade de os dados pessoais por eles fornecidos poderem ser utilizados para um fim diferente daquele para o qual foram recolhidos. O mesmo inquérito revela que 58% estão convencidos de que são obrigados a fornecer informações pessoais para poderem beneficiar de produtos e serviços em linha, enquanto 52% estão céticos quanto ao fornecimento de informações pessoais em troca de serviços em linha (Commission, 2017).

É nossa convicção que os princípios da proteção de dados podem ser introduzidos no desenho ou na análise de um serviço através do uso da Teoria da Atividade, porque esta fornece um método para compreender e analisar um fenómeno, encontrar padrões e fazer inferências através de interações, e de uma linguagem e retórica integradas.

Este artigo está organizado da seguinte forma: Na secção 2 é descrita a nossa motivação para realizar este trabalho. Na secção 3 é feita uma descrição dos trabalhos relacionados nas áreas de serviços, análise de requisitos e Teoria da Atividade. Na secção 4 descreve o conceito de sistema de atividade. Na secção 5 é proposto uma instanciação de um sistema de atividade para a proteção de dados. Por fim na secção 6 é apresentado as conclusões e o trabalho futuro.

2. MOTIVAÇÃO

A complexidade de um serviço é circunscrevida em parte pelo que o sistema faz (i.e. a sua funcionalidade) e em parte pelos requisitos globais sobre desempenho, fiabilidade, capacidade de manutenção, portabilidade, robustez e afins. Estes requisitos não-funcionais, também, mencionados como requisitos de qualidade, porque são requisitos que dizem respeito a uma preocupação de qualidade que não é abrangida por requisitos funcionais. Os requisitos não-funcionais desempenham um papel crítico durante o desenvolvimento do serviço, servindo como critério de seleção para a

escolha entre miríades de conceções alternativas e implementações finais (Chung, Nixon, Yu, & Mylopoulos, 2012).

O RGPD exige a adoção de orientações internas e aplicação de medidas que respeitem os princípios da proteção de dados desde a conceção e da proteção de dados por defeito na fase do desenho e durante a operação de um serviço (Goddard, 2017).

A proteção de dados desde a conceção consiste em considerar previamente as questões de proteção de dados e privacidade na fase de desenho de um serviço e durante a sua existência. Iso requer pôr em prática medidas técnicas e organizacionais adequadas destinadas a implementar eficazmente os princípios de proteção de dados e integrar salvaguardas no tratamento (i.e., operações realizadas com os dados) de modo a satisfazer os requisitos da RGPD e salvaguardar os direitos individuais (Schaar, 2010).

A proteção de dados, por defeito, exige que se assegure que apenas sejam utilizados os dados necessários para atingir o seu objetivo específico. Está ligado aos princípios fundamentais de proteção de dados de minimização de dados e limitação da finalidade. Um serviço tem de manipular alguns dados pessoais para atingir os seus objetivos. A proteção de dados por defeito significa que precisa de determinar estes dados antes do início do tratamento, informar devidamente os indivíduos e manipular apenas os dados de que precisa para os seus fins. Não existe uma solução por defeito. O que precisa de fazer depende das circunstâncias do tratamento e dos riscos colocados aos indivíduos (Danezis et al., 2015).

O nosso objetivo é endereçar a proteção de dados desde a conceção no desenho e na análise da operação de um serviço através da introdução de requisitos de qualidade relacionados com a proteção de dados, tendo em conta a qualidade de utilização de um serviço (i.e., o grau em que um serviço pode ser utilizado por utilizadores para satisfazer as suas necessidades para atingir os objetivos e respeitando os princípios da proteção de dados (McAlexander, Kaldenberg, & Koenig, 1994).

Para alcançar a qualidade de utilização de um serviço, respeitando os princípios de proteção de dados, exige o entendimento partilhado dos objetivos das atividades dos stakeholder e as suas interações com artefactos organizacionais no contexto da Teoria da Atividade

3. ESTADO DA ARTE

O tema da proteção de dados desde a conceção e por defeito tem vindo a ser objeto de investigação. De acordo com a Agência Europeia para a Segurança das Redes e da Informação (ENISA) a Integridade Contextual (IC) de Nissenbaum é um quadro normativo, que na realidade inspirou esta investigação, para modelar o fluxo de informação entre agentes e o raciocínio sobre os padrões de comunicação que causam violações da privacidade (Nissenbaum, 2009).

Basin et al. propõe uma abordagem que identifica os objetivos dos processos, e apresenta um conjunto de modelos formais de comunicação entre processos que podem ser utilizados para auditar e derivar políticas de privacidade (Basin, Debois, & Hildebrandt, 2018).

Diamantopoulou et al. e Zerlang analisaram, do ponto de vista do negócio, formas de formular políticas de privacidade e de cibersegurança de uma forma consistente com a RGPD num esforço para compreender o impacto da regulamentação sobre as receitas e a transação dos dados na UE e no mundo (Angelopoulos, Diamantopoulou, Mouratidis, & Pavlidis, 2017) (Zerlang, 2017).

Drogkaris et al. propõe o uso do Acordo de Nível de Privacidade através de uma arquitetura que promove o emprego de políticas de privacidade e introduz o conceito de agente de controlo de privacidade para armazenar e comparar as políticas de privacidade dos prestadores de serviços e as preferências de privacidade dos utilizadores (Drogkaris, Gritzalis, & Lambrinoudakis, 2013).

Alguns projetos têm investigado a conceção e implementação de sistemas onde abordam a proteção de dados desde a conceção e por defeito, resultantes principalmente de uma perspetiva de engenharia de requisitos, onde a privacidade se torna um problema de conformidade, ou seja, a adesão estrita e formalmente comprovada aos estatutos e regulamentos (Massey, Otto, Hayward, & Antón, 2010).

Uma questão principal ao lidar com requisitos não-funcionais é a sua classificação em alguma taxonomia. Os atributos de qualidade de sistemas podem ser utilizados com esta finalidade. Há muitas propostas, sendo a norma de qualidade ISO/IEC 25010 a mais difundida e permite a especificação dos requisitos de qualidade do serviço e avaliação da qualidade do serviço; apoiado por um processo de mediação da qualidade do serviço. O objetivo é ajudar aqueles que desenvolvem serviços com a especificação e avaliação dos requisitos de qualidade (Estdale & Georgiadou, 2018).

A relação humana com a tecnologia tem sido sempre de especial interesse para a teoria da atividade, o que não é surpreendente dado o foco da teoria na mediação e nos artefactos. Especialmente nos países nórdicos e nos Estados Unidos, salientaram que ao enquadrar a interação das pessoas com os artefactos num contexto mais vasto de atividades humanas, a teoria da atividade permite alcançar uma compreensão mais profunda artefactos, relativamente o seu significado para as pessoas. Notavelmente, Bødker (Bodker, 1989) e Kuutti (Kuutti, 1996) defenderam a adoção da teoria da atividade como base teórica para a interação homem-computador e para o uso na investigação de sistemas de informação. Estes trabalhos e outros trabalhos subsequentes, realizados por Kaptelinin & Nardi, ajudaram a estabelecer a teoria da atividade como uma abordagem teórica fundamental na interação homem-artefacto e foi possível a sua utilização em algumas outras áreas de estudo dentro do campo geral das "pessoas e tecnologia" (Kaptelinin & Nardi, 2012).

Globalmente, uma investigação sistemática do RGPD em benefício dos utilizadores influenciados ainda não está disponível no estado da arte. Por conseguinte, os benefícios e contribuições deste

artigo, de acordo com o enquadramento do GDPR, num serviço enquadrada na Teoria da Atividade são consideráveis.

4. SISTEMA DE ATIVIDADE

Uma atividade é uma forma de realizar tarefas sobre um objeto de modo a atingir um resultado. As atividades distinguem-se umas das outras de acordo com os seus objetivos. A transformação do objeto num objetivo/resultado motiva a existência de uma atividade. Um sistema de atividade é uma representação de uma atividade e é representado como um modelo triangular desenvolvido por Engeström de acordo com a figura 1.

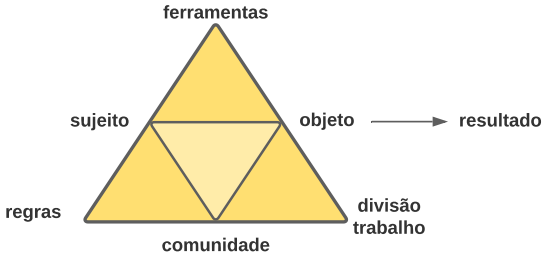

Figura 1 Sistema de atividade de Engeström

Neste modelo existem 6 componentes: O sujeito é o indivíduo ou grupos de indivíduos envolvidos na atividade. A ferramenta inclui artefactos que podem servir como recursos para o sujeito na atividade. O objeto é o objetivo ou o motivo da atividade. As regras são quaisquer regulamentos que, em grau variável, podem afetar a forma como a atividade se desenrola. A comunidade é o grupo social a que o sujeito pertence no âmbito de uma atividade. A divisão do trabalho refere-se à forma como as tarefas são partilhadas entre a comunidade (Engeström & Pyörälä, 2021).

A análise de sistemas de atividade é um método de análise concebido para melhorar a compreensão de atividade humana situada num contexto coletivo, incluindo para isto os conceitos de mediação e de contradições. Segundo Vygotsky as interações dos seres humanos com o seu ambiente não são diretas, mas sim mediadas através da utilização de ferramentas e sinais (VYGOTSKY, 1978).

As contradições referem-se às fontes de influências dentro de um sistema de atividade que podem exercer pressões sobre a atividade. As tensões podem surgir destas pressões e afetar as interações entre os componentes de um sistema de atividade. As tensões podem afetar a capacidade do sujeito de atingir o resultado, assumindo um papel como obstáculo, dificultando o sujeito de atingir o resultado, ou assumindo um papel como uma influência positiva para o sujeito atingir o resultado.

Um sistema de atividade pode ser muito complexo porque pode incorporar várias subactividades que, em conjunto, constituem o principal sistema de atividade em análise. Uma técnica de análise,

introduzida por Mwanza**,** consiste em dividir o sistema de atividade em unidades ou triângulos de menor dimensão (Mwanza, 2001) .

5. PROPOSTA DE UM MODELO DAS PRÁTICAS DE PROTEÇÃO DE DADOS NUM SERVIÇO

Para desenvolver o modelo foi necessário realizar uma análise que começou por interpretar as várias componentes do triângulo de atividade (Figura 1) em termos da situação em análise. Para tal utilizamos o modelo dos oito passos desenvolvido por Mwanza (Mwanza, 2001) e que resulta na tabela apresentada de seguida.

Tabela 1 – Questões em analise.

#	Questão	Requisitos não funcionais
1	Atividade de interesse	Para efeitos do estudo, a atividade de interesse foi identificada como sendo obter os requisitos não-funcionais de segurança dos dados pessoais no contexto de um serviço.
2	Objetivo da atividade	O objetivo ou a finalidade desta atividade é fornecer uma melhor proteção do tratamento dos dados dos clientes.
3	Sujeitos desta atividade	Os sujeitos envolvidos nesta atividade são as pessoas ou grupo de pessoas que trabalham em conjunto numa equipa para prestar o aconselhamento no âmbito do cargo de encarregado da proteção de dados.
4	Ferramentas de mediação da atividade	São as ferramentas que o RGPD proporciona para mediar a interação entre o sujeito e o serviço com o intuito de proteger os dados pessoas.
5	Regras e regulamentos que medeiam a atividade	São regras extraídas dos princípios do RGPD utilizadas na mediação da interação entre o sujeito e a comunidade.
6	Divisão do trabalho que medeia a atividade.	as pessoas que operam o serviço devem cumprir com as regras de proteção e as pessoas que utilizam o serviço podem exercer os seus direitos.
7	Comunidade em que a atividade é conduzida.	A comunidade é constituída pelas pessoas que operam o serviço e as pessoas que utilizam o serviço.
8	Resultado desejado da realização desta atividade	O resultado desejado da realização desta atividade é obter um conjunto de requisitos não-funcionais que permite um equilíbrio entre a operação eficiente de um serviço e a proteção dos dados pessoais.

5.1. Sujeito desta atividade

O sujeito desta atividade é o Encarregado da Proteção de Dados (EPD). O EPD desempenha a responsabilidade de aconselhamento ao responsável pelo tratamento e ao subcontratante, bem como aos trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do RGPD.

O EPD Controla a conformidade com o RGPD e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e as auditorias correspondentes. Tem ainda de prestar aconselhamento no que respeita à avaliação de impacto sobre a proteção de dados (AIEP) e controla a sua realização.

O AEIP deve ser realizado quando um certo tipo de tratamento for suscetível de implicar um elevado risco para os direitos das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais.

5.2. Ferramentas de mediação

As ferramentas são artefactos tecnológicos ou técnicos usados para transformar o serviço e para se chegar ao resultado esperado. As ferramentas alteram e são, por sua vez, alteradas pela atividade, uma vez que medeiam as relações entre o EPD e o serviço. São ao mesmo tempo, um elemento que pode capacitar e limitar o trabalho do EPD. Elas auxiliam o EPD no processo de transformação, mas podem também restringir a interação. No contexto do RGPD são identificadas as seguintes ferramentas: proteção de dados por defeito e desde a conceção, as técnicas de anonimização e as técnicas de pseudonimização.

A proteção de dados por defeito exige que se assegure de que apenas utilize os dados necessários para atingir o seu objetivo específico. Está ligado aos princípios fundamentais de proteção de dados de minimização de dados e limitação da finalidade em simultâneo com a utilização deste modelo o AEIP está também a pôr em prática a proteção de dados desde a conceção, uma vez que estará a considerar as questões de proteção de dados e privacidade na fase de desenho de um serviço.

O uso da anonimização é relevante, em termos de proteção de dados, uma vez que princípios da proteção de dados não se aplicam aos dados tornados anónimos de tal forma que o titular dos dados, ou seja, a pessoa em causa já não seja identificável. O RGPD exige que as entidades que operem os dados pessoais os protejam de uma utilização ou divulgação imprópria. Contudo, as mesmas entidades podem querer, ou podem ser obrigadas, a publicar informação proveniente dos dados pessoais que detêm. Por exemplo, as entidades de serviços de saúde são obrigadas a proteger a identidade de pacientes individuais, mas também podem ser obrigadas a publicar estatísticas sobre

os resultados dos pacientes. A anonimização ajuda as organizações a cumprirem as suas obrigações em matéria de proteção de dados, permitindo-lhes ao mesmo tempo disponibilizar informação ao público.

A aplicação da pseudonimização aos dados pessoais pode reduzir os riscos para os titulares de dados em questão e ajudar os responsáveis pelo tratamento e os seus subcontratantes a cumprir as suas obrigações de proteção de dados. A introdução explícita da «pseudonimização» no RGPD não se destina a excluir eventuais outras medidas de proteção de dados.

5.3. Regras de mediação

As regras de mediação afetam o sentido de desenvolvimento da atividade. As regras podem ser explicitas e implícitas (por exemplo, normas de comportamento social dentro de uma comunidade social especifica). Regras, normas e sanções especificam e regulam, explicita e implicitamente, os procedimentos corretos previstos e as interações aceitáveis entre os participantes dentro do sistema de atividade. No âmbito desta atividade as regras que medeiam a relação entre o Encarregado da Proteção de Dados e a comunidade são:

1. A limitação das finalidades diz que os dados são recolhidos para finalidades determinadas, explicitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades;
2. A licitude, lealdade e transparência indica que deve existir uma razão legal para fazer o tratamento, que devemos transmitir a razão legal, numa linguagem simples, pela qual o tratamento é realizado (lealdade) e não devemos desviar do tratamento inicial a não ser que o titular dos dados autorize (transparência) ou que seja respeitado a limitação das finalidades. Em termos de combinação de licitude, lealdade e transparência o cenário que será mais adequado é aquele em que o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
3. Os dados devem ser mantidos exatos e atualizados por isto devem ser adotadas medidas adequadas para que os dados inexatos sejam apagados ou retificados sem demora;
4. Existe o dever de limitação de conservação dos dados, ou seja, os dados devem ser mantidos de forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados;
5. Devem ser utilizadas medidas técnicas ou organizativas adequadas de segurança contra o tratamento não autorizado e contra a sua perda ou danificação. Isto inclui técnicas de integridade (i.e., correção da informação armazenada e manipulada) e confidencialidade (i.e., restrição do acesso à informação àqueles que estão autorizados;

6 Deve existir transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados. Isto é quando os dados pessoais forem recolhidos junto do titular, o responsável pelo tratamento faculta-lhe, aquando da recolha desses dados pessoais informações sobre o contexto em que os seus dados serão utilizados e os mecanismos de verificação dos mesmos. O mesmo aplica-se quando os dados são recolhidos junto do titular

É de notar que quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais. É de notar que o titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado.

5.4. Comunidade e Divisão de Trabalho

A divisão de trabalho que medeia a relação entre a comunidade e os dados pessoais de um serviço A comunidade é composta pelo responsável pelo tratamento, o subcontratante e o titular dos dados.

O responsável pelo tratamento é a entidade que determine as finalidades e os meios de tratamento dos dados pessoais. Quem determine é identificado ao fazer-se as seguintes perguntas: Qual a finalidade do tratamento? e quem o iniciou? O responsável pelo tratamento é um conceito funcional, que visa atribuir responsabilidade àqueles que exercem uma influência de facto e, como tal, baseia-se numa análise factual e não formal. Ou seja, o responsável pelo tratamento é a entidade que optou por proceder ao tratamento de dados pessoais para os seus próprios fins.

A existência de um subcontratante é uma decisão tomada pelo responsável pelo tratamento em confiar a totalidade ou parte das tarefas de tratamento a uma organização externa. Assim sendo um subcontratante procede ao tratamento de dados pessoais por conta do responsável pelo tratamento. Esta tarefa de tratamento pode restringir-se a um contexto muito específico ou ser mais geral e abrangente. O papel do subcontratante não resulta da natureza de uma entidade que procede ao tratamento de dados, mas sim das suas atividades concretas num contexto específico.

O titular dos dados é uma pessoa sobre a quem os dados podem ser associados, sendo assim considerados como dados pessoais. A definição de dados pessoais refere-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Os titulares dos dados podem exercer os seus direitos junto do responsável pelo tratamento, nomeadamente obter informações sobre as finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento para o tratamento.

A autoridade de controlo contribui para a aplicação coerente do RGPD e neste âmbito trata as reclamações que sejam apresentadas, as eventuais violações do RGPD e promove a sensibilização dos responsáveis pelo tratamento e dos subcontratantes para as suas obrigações nos termos do regulamento. Relativamente aos titulares de dados, se lhe for solicitado, presta informações sobre o exercício dos seus direitos nos termos do regulamento e trata as reclamações apresentadas por estes.

5.5. Modelo das Práticas de Proteção de Dados num Serviço

Com base na análise feita nas seções 5.1 a 5.4 é possível apresentar uma instância de modelo de atividade de Engeström em que atividade é constituída pelas práticas de proteção de dados num serviço (figura 2).

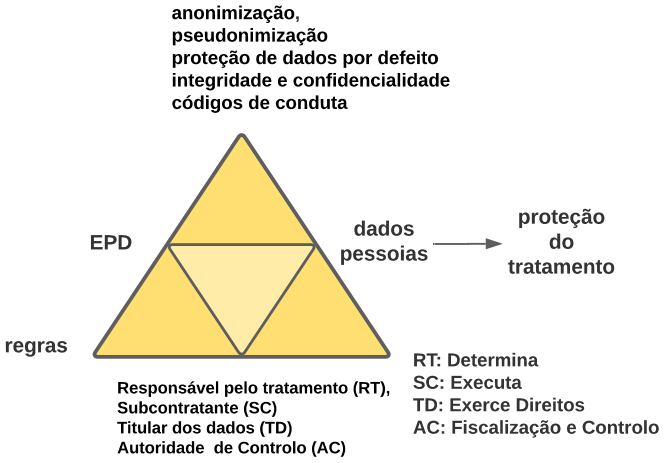

Figura 2. Modelo das práticas de proteção de dados num serviço.

É de notar que embora o objeto de análise seja um serviço, na verdade o foco será nos dados pessoais que são utilizados no serviço, sendo que o resultado esperado é a conformidade com o RGPD, tendo em conta as regras e os papeis desempenhado pelo responsável pelo tratamento, subcontratante e o titular dos dados. Utilizamos para tal os artefactos apresentados no qual incluímos o próprio regulamento.

No contexto da Teoria da Atividade, os sujeitos não interagem com os objetos diretamente, mas sim através da mediação de artefactos que intervêm nesta relação. Entre os artefactos, encontram-se as ferramentas tecnológicas. Na qualidade de artefacto mediador, duas visões podem advir do uso das ferramentas tecnológicas: (1) enquanto artefacto, espera-se que não seja o tema das ações do sujeito, mas sim o seu instrumento. Ou seja, o sujeito não deve ter consciência de estar a manipular uma ferramenta, a não ser que isso seja desejado por quem desenvolve o artefacto e (2) enquanto ferramenta de mediação, a análise das ferramentas o projetista das ferramentas passa a questionar,

além do tradicional: o que o utilizador poderá fazer com as ferramentas? passa a questionar "o que o utilizador e as ferramentas poderão realizar no ambiente que os rodeia?

6. CONCLUSÃO E TRABALHO FUTURO

As práticas e desafios da integração dos requisitos de segurança de informação e proteção de dados nas organizações ainda é uma área relativamente inexplorada de investigação e por isto investigámos o RGPD e mostrámos como é necessário um suporte para relacionar os diversos conceitos do regulamento com o objetivo de demonstrar a sua aplicabilidade num serviço. Para atenuar a questão de que a segurança do tratamento não é normalmente representada explicitamente nos serviços, apresentámos o conceito de associar, no contexto da Teoria da Atividade, o objeto (como sendo um serviço) e um objetivo ou resultado como sendo a proteção de dados. Propusemos uma metodologia em que os conceitos do RGPD são decompostos em conformidade com os conceitos de meadição da Teoria da atividade e os seus pilares: sujeito, comunidade e objeto.

Apresentamos um modelo de práticas de proteção de dados e podemos verificar a conformidade da Teoria da Atividade com os conceitos do RGPD. Em particular, podemos identificar que as regras ou normas medeiam a relação do Encarregado de Proteção com a comunidade (composta pelo responsável pelo tratamento, o subcontratante, o titular dos dados e a autoridade de controlo). Que as ferramentas medeiam a relação do Encarregado de Proteção com o serviço (i.e., o objeto) e por fim que a divisão de trabalho media a relação da comunidade com o serviço.

Este modelo é suficiente abrangente para garantir os aspetos de analise de proteção dos dados pessoais, evitando deste modo os problemas dos modelos mais complexos, composto por conjuntos de regras de acesso complexas. Estes modelos podem levar a pensar que estão a aperfeiçoar a postura de segurança da organização com restrições detalhadas de acesso (princípio do privilégio mínimo), mas fazendo-o também aumenta a possibilidade de cometer um erro de lógica que pode abrir um inesperado buraco no seu perímetro de controlo. Estas são compensações que têm de ser pesadas e feito todos os dias por um EPD.

Como trabalho futuro é nossa intensão analisar como podem ser utilizados os diagramas de atividade para analisar modelos de segurança e proteção de modo a procurar evitar violações nas seguintes circunstâncias: (1) Provocada quando a informação pessoal, combinada com conjuntos de dados externos, pode levar à inferência de novos factos sobre os utilizadores e (2) A informação pessoal é por vezes recolhida e utilizada para acrescentar valor ao negócio. Por exemplo, os hábitos de compra do indivíduo podem revelar muitas informações pessoais como evitar excesso de informação; (3) Como evitar que os dados sensíveis que são armazenados e tratados num local que não possui as medidas de proteção adequadas possam ser sujeitos a fuga de dados durante as várias fases de tratamento e que engloba o tratamento dos dados no ciclo de vida dos dados.

Outro aspeto será obter um equilíbrio entre as medidas de controlo e a ausência delas. Por exemplo, a implementação de controlos de segurança pode introduzir muitas complexidades a uma organização. Estas complexidades podem levar a erros ou dificultar a deteção de atividades não autorizadas e podem por vezes criar uma fraqueza inadvertidamente. Poderemos utilizar os princípios de Saltzer e Schroederh (Saltzer & Schroeder, 1975) para influenciar muitas facetas da segurança, tais como normas, diretrizes, e desenhos de controlo. São eles: privilégio mínimo (não devem ser permitidas comunicações ou atividades a menos que haja uma necessidade explícita para essa transação ou acesso), defesa em profundidade (utilização de múltiplas técnicas de segurança ou camadas de controlos para ajudar a reduzir a exposição se um controlo de segurança for comprometido ou contornado) e separação de privilégios (nenhuma pessoa tem autoridade para desempenhar todas as funções privilegiadas, especialmente todas as funções relacionadas com a criação e tratamento de informação sensível ou crítica).

REFERÊNCIAS

Angelopoulos, K., Diamantopoulou, V., Mouratidis, H., & Pavlidis, M. (2017). A metamodel for GDPR-based privacy level agreements. In *ER Forum/Demos*.

Basin, D., Debois, S., & Hildebrandt, T. (2018). On purpose and by necessity: compliance under the GDPR. In *International Conference on Financial Cryptography and Data Security* (pp. 20–37). Springer.

Bodker, S. (1989). A human activity approach to user interfaces. *Human-Computer Interaction*, *4*(3), 171–195.

Chung, L., Nixon, B. A., Yu, E., & Mylopoulos, J. (2012). *Non-functional requirements in software engineering* (Vol. 5). Springer Science & Business Media.

Commission, E. (2017). Eurobarometer 83.1: Europeans in 2015, Data Protection and the Internet, February-March 2015. GESIS [distributor], Inter-university Consortium for Political and Social Research [distributor]. https://doi.org/10.3886/ICPSR36665.v1

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, D. Le, Tirtea, R., & Schiffner, S. (2015). Privacy and data protection by design-from policy to engineering. *ArXiv Preprint ArXiv:1501.03726*.

Dibble, S. (2020). *GDPR*.

Drogkaris, P., Gritzalis, S., & Lambrinoudakis, C. (2013). Employing privacy policies and preferences in modern e–government environments. *International Journal of Electronic Governance*, *6*(2), 101–116.

Edmond, D., OSullivan, J., & Hofstede, A. ter. (2002). What's in a service? Towards accurate description of non-functional service properties. *Distributed and Parallel Databases*, *12*, 117–133. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.3.7665&rep=rep1&type=pdf

Engeström, Y., & Pyörälä, E. (2021). Using activity theory to transform medical work and learning. *Medical Teacher*, *43*(1), 7–13.

Estdale, J., & Georgiadou, E. (2018). Applying the ISO/IEC 25010 quality models to software product. In *European Conference on Software Process Improvement* (pp. 492–503). Springer.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, *59*(6), 703–705.

Kaptelinin, V., & Nardi, B. (2012). Activity theory in HCI: Fundamentals and reflections. *Synthesis Lectures Human-Centered Informatics*, *5*(1), 1–105.

Kuutti, K. (1996). Activity theory as a potential framework for human-computer interaction research. *Context and Consciousness: Activity Theory and Human-Computer Interaction*, *1744*.

Macaulay, L. A. (2012). *Requirements engineering*. Springer Science & Business Media.

Massey, A. K., Otto, P. N., Hayward, L. J., & Antón, A. I. (2010). Evaluating existing security and privacy requirements for legal compliance. *Requirements Engineering*, *15*(1), 119–137.

McAlexander, J. H., Kaldenberg, D. O., & Koenig, H. F. (1994). Service quality measurement. *Journal of Health Care Marketing*, *14*(3), 34–40.

Mwanza, D. (2001). Where theory meets practice: A case for an activity theory based methodology to guide computer system design.
Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press. Retrieved from https://books.google.nl/books?id=_NN1uGn1Jd8C
Saltzer, J. H., & Schroeder, M. D. (1975). The Protection of Information in Computer Systems A . Considerations Surrounding the Study of Protection. *Access*, *63*(9), 1278–1308. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1451869
Schaar, P. (2010). Privacy by design. *Identity in the Information Society*, *3*(2), 267–274.
VYGOTSKY, L. S. (1978). *Mind in Society*. (M. Cole, V. Jolm-Steiner, S. Scribner, & E. Souberman, Eds.). Harvard University Press. https://doi.org/10.2307/j.ctvjf9vz4
Zerlang, J. (2017). GDPR: a milestone in convergence for cyber-security and compliance. *Network Security*, *2017*(6), 8–11.