UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE EDUCAÇÃO
PROGRAMA DE PÓS-GRADUÇÃO EM TECNOLOGIAS, COMUNICAÇÃO E EDUCAÇÃO

MÁRIO CÉSAR PINTAUDI PEIXOTO

COSI: CONSULTOR ORIENTATIVO PARA A SEGURANÇA DE INFORMAÇÕES EM SMART TV

UBERLÂNDIA
2016

MÁRIO CÉSAR PINTAUDI PEIXOTO

COSI: CONSULTOR ORIENTATIVO PARA A SEGURANÇA DE INFORMAÇÕES EM SMART TV

Dissertação elaborada para a defesa de produto do Mestrado Profissional Interdisciplinar em Tecnologias, Comunicação e Educação da Universidade Federal de Uberlândia.

Orientação: Profa. Dra. Vanessa Matos dos Santos

UBERLÂNDIA

2016

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da UFU, MG, Brasil.

P379c
2017

Peixoto, Mário César Pintaudi, 1980-
COSI : consultor orientativo para a segurança de informações em Smart-TV / Mário César Pintaudi Peixoto. - 2017.
131 f. : il.

Orientadora: Vanessa Matos dos Santos.
Relatório (mestrado profissional) - Universidade Federal de Uberlândia, Programa de Pós-Graduação em Tecnologias, Comunicação e Educação.
Inclui bibliografia.

1. Educação - Teses. 2. Proteção de dados - Teses. 3. Sistemas de recuperação da informação - Medidas de segurança - Teses. 4. Televisão - Inovações tecnológicas - Teses. I. Santos, Vanessa Matos dos. II. Universidade Federal de Uberlândia. Programa de Pós-Graduação em Tecnologias, Comunicação e Educação. III. Título.

CDU: 37

MÁRIO CÉSAR PINTAUDI PEIXOTO

MÁRIO CÉSAR PINTAUDI PEIXOTO

COSI: CONSULTOR ORIENTATIVO PARA A SEGURANÇA DE INFORMAÇÕES EM SMART TV

Dissertação elaborada para defesa de produto do Mestrado Profissional Interdisciplinar em Tecnologias, Comunicação e Educação da Universidade Federal de Uberlândia.

BANCA EXAMINADORA

Participou por vídeo conferência

Prof(a). Dr(a). Francisco Rolfsen Belda
Universidade Estadual Paulista – UNESP

Prof(a). Dr(a). Aléxia Pádua Franco
Universidade Federal de Uberlândia - UFU

Prof(a). Dr(a). Vanessa Matos dos Santos
Universidade Federal de Uberlândia - UFU

Aprovado em: 14/02/2017

RESUMO

Este relatório aborda o desenvolvimento de um aplicativo voltado para a segurança da informação em Smart TVs. No contexto da Internet das Coisas, nem todos estão cientes de que muitas informações de cunho privado podem ser coletadas por meio do aparelho televisivo sem o conhecimento do usuário-telespectador. O aplicativo busca justamente oportunizar esse conhecimento, tornando o cliente da Smart TV menos vulnerável no cenário contemporâneo.

Palavras-chave: Segurança da informação. Privacidade. Smart TV. Internet das coisas.

ABSTRACT

This report addresses the development of an application for information security in Smart-TVs. In the internet scene of things, not everyone is aware that much private information can be collected through the television set without the knowledge of the user and viewer. The application precisely seeks to provide this knowledge to the user and viewer, thus making it less vulnerable in the contemporary scenario

Keywords: Information security. Privacy policies. Smart TV. Internet of things.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AP	Access Point
ARIB	Association of Radio Industries and Business
ATSC	Advanced Television System Committee
BNCC	Base Nacional Comum Curricular
DLNA	Digital Living Network Alliance
DTV	Digital Television
DTVi	Digital Television Interative
DVB	Digital Video Broadcasting
DVI	Digital Visual Interface
DVR	Digital Video Recorder
EC	Consumo de eletrônicos
EFF	Electronic Frontier Foundation
EUDPD	Diretiva da União Europeia de Proteção de Dados
Faced	Faculdade de Educação
FLOSS	Free/Libre and Open Source Software
FOFA	Forças, Oportunidades, Fraquezas e Ameaças
GUT	Gravidade x Urgência x Tendência
HBBTV	Hybrid Broadcast Broadband TV
HDMI	High-Definition Multimedia Interface
HDTV	High-Definition Television
HDCP	High-bandwidth Digital Content Protection
HTPC	Home Theater Personal Computer
HVAC	Heating Ventilating and Air Conditioning
IDC	International Data Corporation
IPTV	Internet Protocol Television
ISDTV	International System for Digital TV
ITU-T	Telecommunication Standardization Sector
IoT	Internet das Coisas
JTAG	Joint Test Access Group
MAC	Média Access Control
MAC	Multiplexed Analogue Component
MHL	Mobile High-Definition Link

MHP	Multimedia Home Platform
MIT	Instituto de Tecnologia de Massachusetts
NTSC	National Television System(s) Committee
OTT	Over-the-Top
PAL	Phase Alternation Line
PBS	Public Broadcasting Service
PowerBox	Decodificador
PC	Personal Computers
PIPEDA	Personal Information Protection and Eletronic Documents
PPGCE	Programa de Pós-Graduação em Tecnologias, Comunicação e Educação
PVC	Polyvinyl Chloride
PVR	Personal Video Recorder
SBTVD-T	Sistema Brasileiro de Televisão Digital Terrestre
SDK	Software Development Kit
SECAM	Séquentiel Couleur à Mémoire
STB	Set Top Box - receptor de TV digital terrestre
Smart TV	TV intelligence
SNS	Social Networking Service
TA	Tecnologia apropriada
TC	Tecnologia convencional
TLS	Transport Layer Security
TS	Tecnologia Social
TVDi	Televisão Digital Interativa
UART	Universal Asynchrounous Receiver Transmissor
UE	União Europeia
UFU	Universidade Federal de Uberlândia
VGA	Video Graphics Array
VoD	Video on Demand
Wi-Fi	Wireless Fidelity

SUMÁRIO

1 APRESENTAÇÃO

A presente pesquisa, inserida no âmbito da linha de pesquisa "Mídias, Educação e Comunicação", do Programa de Pós-Graduação em Tecnologias, Comunicação e Educação (PPGCE) da Faculdade de Educação (Faced) da Universidade Federal de Uberlândia (UFU) aborda a utilização de um recurso comumente doméstico, de comunicação de massa, encontrado em grande parte dos lares, mas também corporativo, porque está presente ainda nas empresas. Este estudo terá, portanto, como foco as chamadas "políticas de privacidade" no contexto da segurança das informações do usuário-telespectador de Smart TV. A proposta é entender o perfil do usuário-cliente, até que ponto ele está à mercê de supostas violações de sua privacidade, bem como saber quais fabricantes deixam públicas suas políticas de privacidade.

Cada fabricante deve manter sempre ao alcance do cliente sua "Política de Privacidade" (chamada por alguns de "Diretiva de Privacidade", "Termos e Condições" ou "Termos de Uso") no que tange à segurança e utilização dos dados pessoais dos usuários. Nessa relação devem constar temas como compartilhamento das informações, esclarecimento de dúvidas referentes a cadastro, *cookies*, enfim, informações que comprovem seu envolvimento e comprometimento para com o cliente. Os termos de serviços nada mais são que o contrato firmado entre o usuário e o fabricante. Ao aceitar o que dizem tais termos, o usuário confirma estar de acordo com cada linha escrita no documento que se pressupõe que tenha lido.

Este relatório esclarece os diferentes aspectos de construção teórica e metodológica do plano de aplicação apresentado. Em primeiro lugar, está esboçado o memorial descritivo que, segundo Oliveira (2005, p. 121), "é um depoimento escrito relativo à lembrança, à vivência de alguém; memórias. Deve conter um breve relato sobre a história de vida pessoal, profissional e cultural do memorialista. Por isso mesmo é escrito com o uso da primeira pessoa". Com este memorial pessoal-profissional, o pesquisador reforça que o interesse pelo desenvolvimento do projeto é resultado de sua própria história de vida, de sua formação acadêmica e profissional. Em seguida, é apresentado o tema e problema de pesquisa, sua importância para a área, além do objetivo geral e dos específicos.

A estrutura do relatório será basicamente formada pela temática e objeto de estudo, com os objetivos a serem cumpridos. Ele se justifica por construir e trazer este produto. A fundamentação teórica é feita no capítulo 1, junto à Introdução. O capítulo 2 demonstra a

importância das políticas de privacidade relativas à segurança das informações e faz o levantamento das que são fornecidas por cada fabricante de Smart TV, além de apontar seus reflexos no que se refere à segurança da informação do usuário. No capítulo 3 apresentam-se algumas detecções de vulnerabilidades em Smart TVs e é feita uma análise de suas ameaças, riscos e impactos. Os dados do produto, seu plano de aplicação e a pré-produção que compõem o projeto serão evidenciados no capítulo 4. Já no capítulo 5 serão apresentados os procedimentos metodológicos, seus métodos e técnicas, além de uma breve descrição da plataforma de desenvolvimento e dos requisitos de sistema necessários, bem como as etapas de desenvolvimento do projeto para a formação e o embasamento das ideias, trazendo um *use-case* (caso de uso) e sua aplicabilidade, com apresentação do plano de aplicação do modelo de negócios Canvas. Por fim, o capítulo 6 esclarece a exequibilidade e aplicabilidade do plano de aplicação, com apresentação do cronograma, dos custos e da matriz SWOT do projeto apresentado. E no capitulo 7, as conclusões finais.

1.1 Memorial acadêmico

Em 1996 iniciei minhas primeiras experiências no mercado de trabalho da área da informática como digitador nos computadores da Central de Cadastro Pessoal de Clientes das Lojas MIG. Em seguida, trabalhei na empresa financeira Fininvest com registro cadastral de documentos, e depois na Asbace, na compensação de cheques. Consegui mais tarde um trabalho temporário na Justiça Eleitoral como técnico em sistemas de urnas eletrônicas. Em 2000, entrei para o Centro Universitário do Triângulo, no curso de graduação em Ciência da Computação. Em paralelo, comecei um estágio como desenvolvedor na Cedro Sistemas. Comecei a atuar profissionalmente em 2003, como analista e supervisor de suporte na Uniube. Lá fiquei durante seis anos. Nesse período obtive a certificação ITIL-Foundation.

Em 2004 tornei-me bacharel em Ciência da Computação, e no ano seguinte fiz uma especialização em Segurança da Informação na Uniminas. Em seguida terminei o MBA em Gestão de Projetos pela Fundação Getúlio Vargas. Recebi então um convite para trabalhar na CTBC do grupo Algar como analista de inovação em TI e segurança da informação.

Nesse período fiz a certificação em *Information Security* and *Foundations Cloud Computing Architecture* V1 (ISO/IEC 27002) pela IBM. Posteriormente, iniciei atividades na área acadêmica como professor do curso de Sistemas de Informação e Engenharias da Uniube. Desejando novos desafios, em 2012 trabalhei como coordenador de Segurança da Informação na multinacional russa Sodrugestvo, em uma filial em Orlândia-SP, e em seguida

em Uberlândia-MG durante quase um ano. Em seguida exerci a atividade de coordenador/gestor do Service Desk da Callink Serviços de Call Center do grupo Arcom durante três anos, período no qual tirei a certificação ISO/IEC 20000 - IT *Service Management*. Continuei em paralelo a ministrar aulas na Faculdade Pitágoras, na pós-graduação em Segurança da Informação e Gestão de TI, bem como na graduação, em Sistemas de Informação e Redes de Computadores. Trabalhei também como Instrutor de treinamentos da Zillion e fui colaborador TM Forum nas frentes *Fraud Operations Managemente Security Management*.

Atualmente sou membro do Comitê Brasileiro sobre as Normas de Gestão de Segurança da Informação (ABNT/CB21) da série 27000. Sou escritor/autor de livros na área de Tecnologia, Segurança e Governança de TI, colunista do WebInsider da Uol e blogueiro do InfoBlog no Jornal Correio.

Em março de 2015, com muito sacrifício (e o auxílio da Profa. Dra. Adriana Omena, que sempre me incentivou a não desistir), finalmente consegui ingressar no Programa de Pós-Graduação do Mestrado Profissional em Tecnologias, Comunicação e Educação da UFU, no qual, no primeiro semestre, cursei disciplinas como Fundamentos Epistemológicos e Educomunicação. No segundo semestre, as disciplinas escolhidas foram Procedimentos Metodológicos de Pesquisa e Tópicos Especiais em Educação e Tecnologia, que agregaram um grande embasamento para a minha formação e me proporcionaram uma visão mais ampla dos domínios metodológicos em educação em mídias e comunicação. Com isso, ocorreu uma sinergia entre minha experiência profissional e o meio cientifico e de pesquisa laboral, solidificando-se um "coeficiente comum" entre a segurança da informação e o meio midiático, educacional e comunicativo, o que proporcionou o fomento para que eu construísse um trabalho junto com minha orientadora, a Profa. Dra. Vanessa Matos dos Santos, que culminou numa relação das televisões digitais inteligentes com foco no processo de segurança das informações do usuário-cliente inerentes ao contexto das políticas de privacidade de cada fabricante de Smart TV.

Neste sentido, participando como um dos agentes responsáveis pelos processos de segurança nas diferentes empresas pelas quais passei e vivenciando as melhores práticas, acompanhando as vulnerabilidades e ameaças a que o usuário de Smart TV está exposto em diferentes ambientes, percebi, junto com minha orientadora, uma grande oportunidade de explicitar como o usuário-cliente, sobretudo no panorama da Internet das Coisas, torna-se vulnerável ao utilizar cada vez mais tal meio de comunicação de massa, seja dentro da empresa onde trabalha, seja em sua própria residência.

1.2 Introdução

Com o passar do tempo e a evolução da tecnologia, atualmente o modelo mais simples de TV é, literalmente, uma TV inteligente, com recursos avançados de interação e interface homem-máquina. Com a inclusão digital[1], o acesso a esses tipos de equipamento se expande cada vez mais entre as diversas classes sociais. Toda essa interação, acessibilidade, mobilidade e a facilidade na transposição dos conteúdos digitais de diferentes equipamentos para a Smart TV faz com que a segurança das informações do usuário seja um desafio a ser enfrentado por ele, bem como pelo próprio fabricante desse tipo de equipamento. Toda essa nova dinâmica em torno da Smart TV faz pensar no nosso comportamento, atitude e reação perante tanta informação e interação, num contexto em que se é ao mesmo tempo espectador (usuários que assistem à Smart TV) e protagonista (cliente que define a necessidade de consumo e aceita as políticas de privacidade do fabricante). É com relação a essa interface cultural que Steven Johnson revela sua preocupação:

> A interface é uma maneira de mapear esse território novo e estranho, um meio de nos orientarmos num ambiente desnorteante. Décadas atrás, Doug Engelbart e um punhado de outros visionários reconheceram que a explosão da informação poderia ser tanto libertadora quanto destrutiva – e sem uma metaforma para nos guiar por esse espaço-informação, correríamos o risco de nos perder no excesso de informação. (JOHNSON, 2001, p. 33).

Sabe-se que existem outras vertentes que levam a pensar no conceito de televisão-inteligente, por exemplo, quando se fala em HbbTV, Set Top Box, PowerBox, PVRs, VoD ou IPTV (cf. lista de abreviaturas e siglas). No entanto, vamos centrar nosso estudo na Smart TV.

Cabe aqui uma pequena reflexão sobre uma situação real que pode vir ocorrer: a partir do momento em que uma TV tem Wi-Fi integrado/embutido, sendo conhecida também como "internet-tv" (o adaptador do televisor é capaz de captar o sinal Wi-Fi), alguns perigos iminentes podem vir à tona, uma vez que é extremamente normal controlar esse tipo de televisão por meio de aplicativos para smartphones.

A comodidade de ter Wi-Fi integrado sem precisar plugar um adaptador (parecido com um pen drive) na TV pode significar um descuido com a segurança das informações do usuário. A partir do momento em que a TV esteja configurada para detectar o *Access Point*

[1] Chamamos de inclusão digital a tentativa de garantir a todas as pessoas o acesso às tecnologias de informação e comunicação (TICs). A ideia é que todas as pessoas, principalmente as de baixa renda, possam ter acesso a informações, fazer pesquisas, mandar e-mails e mais: facilitar sua própria vida fazendo uso da tecnologia. Cf. - http://www.infoescola.com/educacao/inclusao-digital/.

(AP) ou roteador wireless automaticamente quando ligada, o usuário estará, portanto, literalmente on-line, o que pode ser perigoso. Entretanto, o próprio manual do usuário das televisões não menciona esse tipo de situação. O importante para o fabricante é que o usuário-telespectador ligue e utilize sua Smart TV, independentemente de qualquer processo preventivo.

Alguns dicionários (Michaelis[2], Aurélio[3]) apresentam o seguinte significado para a palavra "privacidade": condição do que é pessoal, íntimo, vida privada, intimidade, privacidade. Intimidade de pessoal ou grupo de pessoas.

O conceito de privacidade nasceu na filosofia antiga, com a distinção entre público e privado, como demonstra a dicotomia aristotélica (Aristóteles, 1988, p. 12) entre vida política, na polis, e doméstica, na oikos[4].

> Até a primeira metade do século XIX a defesa do direito à privacidade confundiu-se com a da propriedade privada e da honra, mas a partir da segunda metade do século XIX a tutela da privacidade recebeu novos contornos na América e na Europa. No século XX, as inovações tecnológicas provocaram súbitas mudanças de paradigmas e de formatação no conceito de privacidade, elevando o risco da violação do direito a graus continuamente mais elevados, conforme o desejo de obter informações sobre pessoas tornou-se crescente a grupos econômicos e políticos, conhecedores de que quem detém a informação detém o poder (e o lucro). Esta correlação foi apontada por J. Oliveira Ascensão ao observar que o período seguinte à guerra do Vietnam, mostrando-se oportuno o surgimento de uma alternativa ao poderio nuclear, essa foi encontrada na informação, de sorte que "[...] o grande lema (que não foi dito) passaria a ser: "Quem domina a informação domina o mundo" (NAVARRO; LEONARDOS, 2011, p. 4).

O cientista da informação Rainer Kuhlen (2004) concebe o conceito de "privacidade" (*Privatheit*) não apenas como proteção de dados ou como o direito de ser deixado em paz, mas também como "autonomia informacional" (*informationelle Selbstbestimmung*), ou seja, a capacidade de escolher e utilizar o conhecimento e a informação autonomamente em um ambiente eletrônico, e de determinar quais atributos de si serão usados por outros (KUHLEN, 2004).

Na segunda metade do século XIX, foi declarada a autonomia da *privacy* em relação ao direito de propriedade, independência obtida por meio de sucessivos julgamentos da

---

[2] Cf. http://michaelis.uol.com.br/busca?id=po13w.
[3] Cf. https://dicionariodoaurelio.com/privacidade.
[4] Esfera digna de proteção, como também pareceu aos romanos. A esse respeito disse o juiz J. Cobb, da Suprema Corte da Geórgia, no julgamento de Pavesich v. New England Life Insurance CO. et al: "*Under the Roman law, 'to enter a man's house against his will, even to serve a summons, was regarded as an invasion of his privacy.' Hunter's Roman Law (3d ed.), 149. This conception is the foundation of the common-law maxim that 'every man's house is his castle'...*". Cf. Georgia (1904).

Suprema Corte norte-americana, mas que teve, como início de caminhada, o célebre ensaio assinado pelos advogados Samuel D. Warren e Louis D. Brandies publicado na *Harvard Law Review* de dezembro de 1890, intitulado *The Right to Privacy* (WARREN; BRANDEIS, 1890). Os ensaístas mencionaram a transformação da sociedade por força das mudanças econômicas e políticas que agitavam aquele fim de século XIX, e fizeram a análise de vários julgamentos dos tribunais americanos, e da inteligência das decisões e dos princípios que as fundamentaram extraíram a ideia de um direito autônomo em relação ao de propriedade, a que denominaram *right to privacy.*

> Warren e Brandeis direcionaram as tratativas para o foco sobre informações da vida privada. De maneira que havia na época o desenvolvimento das técnicas de impressão, o emprego da fotografia – a captação à distância das imagens de pessoas sem permissão estampando a imprensa diária, bem como a rápida divulgação da notícia, que faria assim o alerta aos "homens da lei" quanto à inevitável transformação em curso, o que gerava de certa forma uma ameaça aos vigentes valores morais e políticos. Sobre o direito à privacidade e direito de exercer controle da informação sobre si, vale resgatar o famoso ensaio de Warren e Brandeis que já espelhava, naquele fim de século XIX, a nítida preocupação quanto à divulgação não consentida de informações relativas à intimidade da vida privada, já com as invenções da época que permitiam mais agilidade na captura de dados pessoais (a imagem, por exemplo, através do daguerreotipo) e divulgação destes (máquinas de tipografia mais ágeis à impressão de jornais e novos meios de transporte), o que gerava por outro lado, a construção de mecanismos jurídicos que se mostrassem hábeis à repressão de condutas invasivas ou à prevenção de riscos (NAVARRO; LEONARDOS, 2011, p. 5).

A verdade é que as Smart TVs atualmente, que não possuem uma política de privacidade, além de não mencionarem que vão assegurar as informações do usuário, podem fazer o que bem quiserem com elas caso sua segurança não esteja legalmente firmada/compactuada. Outro fator importante é que o recurso *Digital Living Network Alliance* (DLNA)[5], apesar de ser bom, prático e interessante por permitir transferências de fotos, imagens, sons e arquivos do dispositivo móvel ou de qualquer outro equipamento para a Smart TV, deve ser utilizado com cautela, uma vez que, ao estar on-line (na internet), o usuário, dependendo da política de privacidade da empresa, pode ter suas informações/arquivos compartilhados enviados para o fabricante ou para outras fontes.

---

[5] A **DLNA** (tradução livre: Aliança para Redes Domésticas Digitais) é uma organização constituída por empresas associadas com a finalidade de estabelecer diretrizes baseadas em padrões tecnológicos já existentes, objetivando garantir a interoperabilidade entre eletrônicos conectados em uma rede doméstica de modo que estes possam trocar arquivos de mídia entre si utilizando a rede em questão, ou seja, o usuário seria capaz de acessar e reproduzir arquivos de mídia de um computador, por exemplo, por intermédio de uma TV, um *tablet*, um smartphone, entre outros aparelhos, desde que estes se encontrem conectados na mesma rede (DLNA, 2015).

Vale ressaltar neste momento que a "política de privacidade" é um conjunto de regras que deve ser fornecido ao usuário pela empresa e que determina como serão utilizadas as informações fornecidas pelos usuários, devendo funcionar como uma espécie de garantia para que estes saibam que seus dados serão protegidos.

Tomando-se como base que um conjunto de dados coerentes fornece informações que, ao serem convertidas em conhecimento, posteriormente auxiliam nas tomadas de decisão, percebe-se o quão estrategicamente a coleta de tais informações (uma vez compiladas de voz para texto, por exemplo) serve como um "arcabouço" de sustentação para formar uma base de dados interessantes. Neste cenário temos as televisões inteligentes, que podem ter acesso às informações do usuário muitas vezes sem tomar os devidos cuidados, pois, visto que muitos fabricantes não fornecem ou não deixam claras suas políticas de privacidade, não se sabe se as palavras do cliente foram transmitidas por meio de um formulário seguro (criptografado), permitido/respaldado por tais políticas. Seria necessário saber ainda se há algum mecanismo de proteção da Smart TV quanto ao acesso indevido quando ela está on-line, por exemplo, a exigência de um processo de autenticação ou de identificação por MAC ao se verificar a tentativa de invasão de algum dispositivo externo ao ambiente da Smart TV.

Conforme reportagem de Helton Simões Gomes e Cristiane Caoli, traga pela pesquisa do IBGE, a única forma de ver TV para 54,5% dos domicílios com televisores no Brasil é por meio de um aparelho ultrapassado, como a TV de tubo (GOMES; CAOLI, 2015). Esta já não é mais fabricada pela indústria brasileira segundo a Eletros (Associação dos Fabricantes de Eletroeletrônicos). Os itens restantes estão somente nos estoques das lojas. Outro fator interessante é que o Ministério das Comunicações tem analisado de que forma o desligamento do sinal analógico, em 2018, poderá impactar os brasileiros. A meta da pasta é levar o sinal para, no mínimo, 93% das residências que recebem programação de TV aberta com antenas analógicas. Quem sabe então haverá assim, nas próximas décadas, um "boom" de conversão forçada para Smart TV de todas as classes sociais.

Além da segurança pública e de Estado, que sempre estimulam a criação das normas de proteção de dados pessoais, tanto nos Estados Unidos da América como na União Europeia há outros componentes que, em conjunto, propiciam uma maior ou menor proteção da privacidade em dado espaço e tempo. A questão cultural serve à investigação com relação às normas de proteção dos dados pessoais dos modelos norte-americano e brasileiro de coleta de desses dados para fins de investigação criminal, considerando, por exemplo, que as interceptações telefônicas judicialmente autorizadas ficam sob gerenciamento das autoridades americanas e brasileiras. O mais recente relatório oficial americano disponível a respeito

(*Wiretap Report*) encerrou o seu período de apuração em 31 de dezembro de 2010, registrando um aumento do número de escutas federais e estaduais de 34%, ou seja, 3.194 escutas num tempo médio de 29 dias (em 2009 foram 2.376 escutas). Se esses números impressionam num primeiro momento, mostram-se tímidos, porém, quando comparados aos do Brasil, onde, apenas em março de 2010 – para situar a comparação entre os dois países em período próximo no tempo – havia mais de 10 mil escutas telefônicas autorizadas judicialmente.[6]

Em uma época na qual a questão da transparência das deliberações públicas segue prestigiada por legislações que visam conferir melhores práticas institucionais para a garantia dos direitos fundamentais, torna-se necessário um mais amplo debate nacional no que tange refere à privacidade das informações pessoais, à sua coleta e manejo pelo poder público e empresas privadas, à sua comunicação a terceiros, à finalidade dos atos de tratamento de dados, aos direitos e às garantias dos cidadãos e a outras questões correlatas. Sobretudo agora, que estamos cada vez mais integrados, conectados numa espécie de bolha da falta de privacidade, neste mundo chamado Internet das Coisas.

1.2.1 Objetivos

1.2.1.1 Geral

Desenvolver um aplicativo mobile para dispositivos Android, de forma que o usuário possa instalá-lo em seu celular e ter condições de, até mesmo antes de efetuar a compra de uma Smart TV de certo fabricante, obter acesso à informação e a esclarecimentos sobre tal aparelho e suas políticas de privacidade.

1.2.1.2 Específicos

Destacar as principais informações que cada política de privacidade pode colher do usuário, bem como demonstrar quais dos fabricantes existentes no mercado possuem, de fato, uma política de privacidade definida, além de:

a) caracterizar os tipos de usuários-telespectadores que utilizam Smart TVs;

b) identificar vulnerabilidades em Smart TVs.

---

[6] A respeito, cf. a notícia disponível em: http://www.conjur.com.br/2010-mai-23/cnj-revela-brasil-105-mil-interceptacoes-telefonicas-curso Acesso em: 12 jun. 2015.

1.2.2 Hipóteses

O usuário, como um cliente-telespectador que adquire uma Smart TV, aceita as condições de uso do produto sem a plena e devida conscientização de que o fabricante poderá absorver informações com base em sua política de privacidade, e não possui sequer um mecanismo que lhe possibilite uma conduta preventiva de consulta e educação informativa a respeito de tais políticas (isso no caso das empresas que a possuem). Vale ressaltar que o usuário desse tipo de equipamento muitas vezes não percebe de imediato que a segurança de suas informações está em jogo.

1.2.3 Público-alvo

O público-alvo primário que poderá usufruir do produto proposto por este trabalho, conforme sua condição socioeconômica, é o próprio cliente que pretende adquirir uma Smart TV e que será, consequentemente, seu usuário.

Por outro lado, de forma secundaria, tal produto acaba sendo útil também para o próprio fabricante, que poderá ter um software capaz de centralizar todas as políticas de privacidade atuais de cada tipo de Smart TV num único lugar, facilitando a consulta para o usuário-cliente.

1.3 Justificativa

Possuímos nos tempos atuais uma metamorfose dos dois meios de comunicação de massa mais poderosos do mundo, a TV e a Internet, transformação essa unificada, mas que não vem sendo percebida. A internet incorpora o acesso à TV e a Smart TV incorpora o acesso à internet. (TVCOMINTERNET, 2016)

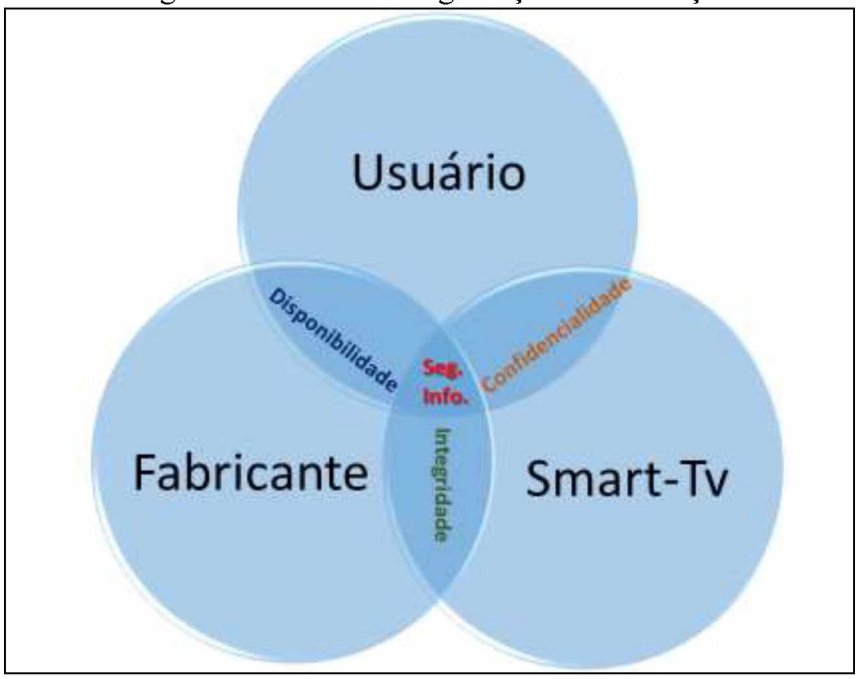
A pequena, mas importante diferença, é que um PC que se adquire nem sempre fica às margens do território do fabricante, diferentemente de quando se compra uma Smart TV, em que todo o Sistema Operacional, firmware, a arquitetura da televisão está direcionada para segmentar os dados ao seu interesse de captação.

Por isso, mais do que nunca, conhecer os interesses do fabricante se faz importante, de maneira que eles deveriam estar mencionados na política de privacidade de cada empresa que fabrica Smart TV.

Todavia, raramente as políticas de privacidade são publicadas por todos os fabricantes e, quando isso ocorre, não estão facilmente disponíveis ou encontráveis, sendo piores os casos em que elas não existem. Tal situação impossibilita que o cliente-usuário que adquiriu sua Smart TV tenha exato conhecimento do quanto seus dados pessoais podem estar vulneráveis e serem captados e absorvidos. Se antes de adquirir sua Smart TV ele tivesse algum recurso que pudesse consultar, poderia melhor se informar antes de tomar a decisão de compra.

Seria um diferencial de consulta técnica, legal e de segurança, um verdadeiro benefício social, possibilitar um recurso capaz de centralizar as políticas de privacidade num único local de acesso que permitiria saber da existência ou não das políticas de privacidade de cada tipo de fabricante, com a possibilidade de conhecer tais políticas. Outro ponto importante é que tal recurso facilitaria o acesso aos jargões, às nomenclaturas e às siglas do universo das Smart TVs, além de esclarecer dúvidas e desafiar os conhecimentos do usuário a respeito do mundo da segurança das informações.

Figura 1 – Pilares da Segurança da Informação



Fonte: Pesquisa/Elaboração do próprio autor.

Neste contexto, passa a ser importante o entendimento do cenário que envolve o fabricante, o usuário e a Smart TV no que se refere aos pilares da segurança da informação

representados pela confidencialidade, integridade e disponibilidade, conforme apresentado na Figura 1. Confidencialidade no sentido de que o usuário pode ter a certeza de que as suas informações pessoais serão transmitidas tão somente para o fabricante de sua Smart TV, e com o seu consentimento, após aceitar a politica de privacidade da empresa. Integridade no sentido de que tais informações (idas e vindas) não venham a ser alteradas no decorrer desse tráfego, e disponibilidade no sentido de que o usuário possa dispor das informações inerentes ao seu contexto sempre que necessário. Dessa maneira, o cliente-usuário poderia ter à sua disposição recursos e informações em sua Smart TV sempre que as solicitasse, bem como poderia navegar, transmitir e compartilhar informações de forma integral, sem a alteração de seus dados, com a confiança de que aquilo que está em trânsito seguirá para o destino real objetivado por ele ao partir de sua Smart TV.

Em uma pesquisa feita no portal da Capes Periódicos foram encontrados 7.583 resultados para a palavra *Smart TV*. Ao pesquisar sobre *Security Smart TV*, 196 foram os resultados encontrados. Já realizando a busca por *Privacy Policy Smart TV,* encontraram-se 10 resultados, sendo 4 mais especificos e coerentes com o assunto. Ao se buscar o termo *televisão inteligente* não se encontraram referências que designassem o aparelho em si, bem como, ao se pesquisar *política privacidade televisão* também não foram encontradas referências mais pontuais ao assunto na língua portuguesa.

Existem, de fato, trabalhos sobre a preocupação do usuário em relação à segurança de suas informações quando utiliza a Smart TV. Mesmo ainda de forma incipiente, há boas pesquisas sobre vulnerabilidades, mas ainda com caminhos a serem percorridos junto com os fabricantes. Todavia, há poucos trabalhos e pesquisas que tratem das políticas de privacidade das Smart TVs no que se refere justamente à segurança das informações fornecidas pelos usuários. Por isso, uma melhor exploração deste assunto se fortalece ainda mais, pois poderá contribuir para sanar as ameaças e vulnerabilidades e para possibilitar contramedidas capazes de mitigar os riscos existentes.

2 A SMART TVS E AS POLÍTICAS DE PRIVACIDADE

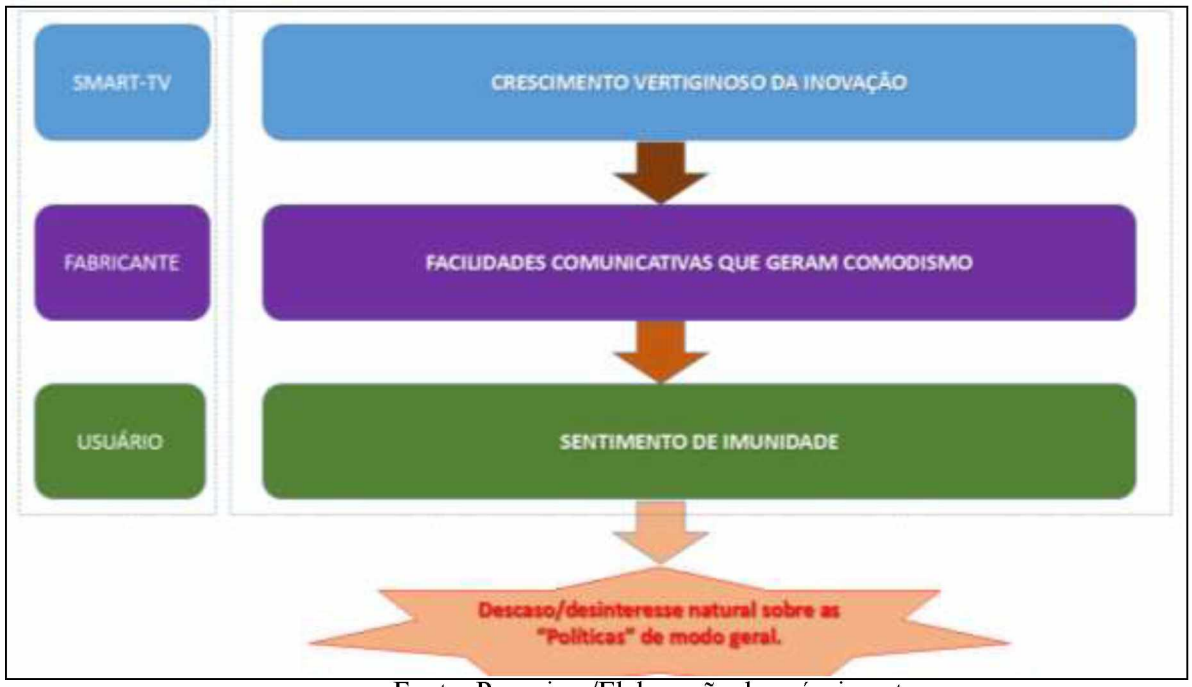
A palavra televisão vem do grego *tele*, "distante", e do latim *visione,* "visão", representando um sistema eletrônico de recepção de imagens e som de forma instantânea (JWSAT, 2015). A televisão funciona por meio da análise e da conversão da luz e do som em ondas eletromagnéticas e de sua reconversão em um aparelho – o televisor – que recebe o mesmo nome do sistema ou pode ainda ser chamado de aparelho de televisão (ELO, 2016).

Acaba sendo comum que raramente lembremos o nome do inventor da televisão, tão facilmente como muitas vezes nos lembramos o do telefone (Graham Bell) ou da lâmpada (Thomas Edison). De certa forma, existe uma razão até simples para tal fato: aquilo que atualmente conhecemos como "aparelho televisivo" é o resultado ou a combinação de muitas invenções de diferentes inventores de períodos e locais diferentes. Contudo, existe um inventor que merece o mérito de ser um dos pioneiros, senão o grande "pai" da televisão, o escocês John Logie Baird (2014).

Com a chegada da TV digital, indaga-se qual seria a diferença entre esse novo modelo de TV e as tradicionais e antigas televisões de tubo, que habitualmente utilizávamos nas casas de nossos pais e avós. No entanto, temos percebido cada vez mais a singularidade da nova TV digital em relação aos computadores, visto que a imagem e som da primeira são digitalizados. Temos consequentemente claros benefícios com as imagens em alta definição, o som de melhor qualidade e aplicações cada vez mais interativas que proporcionam uma experiência mais rica e abrangente ao telespectador.

A relação do homem com a tecnologia, segundo Vieira Pinto (2005), deve ser vista de duas maneiras, por intermédio do maravilhamento e da dominação tecnológica. O homem primitivo maravilhava-se com os fenômenos da natureza. O homem metropolitano moderno maravilha-se, sobretudo, com objetos tecnológicos, em virtude de uma "ideologia" que o faz acreditar que vive num mundo magnânimo e progressista. Vejamos na Figura 2 como essa visão de Vieira Pinto pode ser transposta para o cenário de hoje, no contexto que estamos estudando.

Figura 2 – O desinteresse pela Política de Privacidade



Fonte: Pesquisas/Elaboração do próprio autor.

A Figura 2 divide-se em dois espectros de entendimento: temos, de um lado, os agentes participantes do processo (Smart TV, fabricante e usuário), e do outro as consequências e os efeitos que a tecnologia em si traz. Neste contexto, há um fato que vivenciamos em nossa sociedade atual: o vertiginoso crescimento da inovação tecnológica. Este traz consigo a evolução do aparelho televisivo, sendo que temos hoje o que há de melhor: a **Smart TV**, que possibilita facilidades comunicativas que geram o comodismo. Facilidades essas que o próprio **fabricante** desenvolve, com suas características de comunicação, integração e interação em benefício do usuário-cliente. Vale aqui destacar que entre os dois agentes citados prevalece a transparência da informação e de todo o processo comunicacional sem a percepção do seu usuário, indo ao encontro do que Vieira Pinto chama de dominação tecnológica. Por fim, as comodidades propiciadas pela Smart TV trazem a existência de um certo sentimento de imunidade, previsto também por Vieira Pinto e denominado de maravilhamento, levando ao descaso e ao desinteresse natural do usuário, cliente, cidadão em relação às normas e diretrizes existentes, ou seja, no nosso caso específico de estudo, as políticas de privacidade.

Esse é um dos grandes "perigos" que o crescimento vertiginoso da inovação traz, pois o alto teor de tecnologia oferecido pelos fabricantes neste mundo da Internet das Coisas e da realidade aumentada possibilita grandes facilidades comunicacionais, de interação e integração. São tantas as facilidades e atrações que esse "encantamento enfeitiçado" induz o

usuário a não perceber tais perigos, mascarados de certa forma por todo o entretenimento revolucionário de um mercado cada vez mais consumista, que busca levar ao usuário este quarteto dos "is": inovação, interação, integração e inteligência.

Um bom exemplo prático e recente é o atual jogo *Pokémon Go*, uma vez que o aplicativo exige acesso total às informações de quem usa a conta do Google para acessar o game, impedindo a privacidade do usuário. Especialistas em segurança expressaram preocupação com a versão no iOS do aplicativo da Nintendo após descobrirem que ele exige que os usuários deem total acesso a suas contas no Google. Tal nível de permissão possibilita ao aplicativo alcance irrestrito a uma quantidade imensa de informação, incluindo e-mail do usuário, calendário, mapas, histórico de localização e basicamente tudo que esteja associado à conta do Google. Além da preocupação com a privacidade, há ainda uma potencial ameaça à segurança. Isso porque a possibilidade de leitura e envio de e-mails permite o acesso a informações ainda mais pessoais do usuário (POKEMON GO..., 2016). O interessante neste contexto é a aplicabilidade do processo de "gamificação" como forma de utilizar certas mecânicas e dinâmicas de jogos para engajar as pessoas (no caso da Smart TV, os seus usuários), resolvendo problemas e melhorando sobretudo o aprendizado no que concerne às questões relativas às políticas de privacidade, por exemplo, motivando suas ações e comportamentos em ambientes fora do contexto de jogos, ou seja, no mundo real. Isso ocorre porque o *gamification* nada mais é que a estratégia de interação entre pessoas e empresas com base no oferecimento de incentivos que estimulam o engajamento do público com as marcas de maneira lúdica.

O aparelho televisivo é sem dúvida um dos produtos que mais se consagrou em sua mutação na sociedade do século XX. O *design* da TV se transformou muito desde as antigas TVs de tubo, como o Emyvisor e o Marconi. No entanto, a informação que chega à tela da nossa TV passa por fios ou cabos, e nós consumimos o que as redes de televisão decidem que nós devamos consumir. O único mecanismo de feedback que temos é o controle remoto (a maior parte da "filtragem de informação" ainda é do tipo mudança de canal.)

A metamídia, que de fato consegue deslizar até a tela, é apenas um expediente (JOHNSON, 2001). Essa colocação de Steven Johnson é bastante pertinente, contudo, nos dias atuais, um pouco dessa realidade de dependência total do controle remoto para a mudança de canal, com a filtragem da informação ainda contida nos canais preestabelecidos de uma dada programação, o que nos deixa encarcerados nesse expediente, de certa forma mudou. Se, por um lado, tivemos certa evolução nesse contexto mais dinâmico com a chegada

das Smart TVs, por outro, ainda estamos atrasados no que se refere ao acompanhamento dessa evolução por parte das políticas de privacidade.

Quadro 1 - As três gerações de TV

Características	Primeira geração (fordista)	Segunda geração	Terceira geração
Serviços	Limitada quantidade de serviços unidirecionais de radiodifusão massiva	Grande quantidade de serviços unidirecionais de radiodifusão segmentada	Serviços e interatividade de radiodifusão e telecomunicações
Modelo de negócios	Publicidade massiva e/ou subsídio governamental	Publicidade segmentada e assinaturas	Publicidade segmentada, assinaturas e pagamento por uso de serviços
Estratégia de negócios	Direitos de propriedade sobre o espectro	Integração vertical entre distribuidores e programadores	Controle de acesso e normas proprietárias no decodificador
Modelo de regulação	Serviço público com proteção aos concessionários	Serviço privado com certas obrigações públicas	Ainda não definido

Fonte: Montez e Becker (2005, p. 77)

Com a possibilidade, atualmente, de se utilizar um conversor Set top Box[7], consegue-se ter acesso à transmissão digital mesmo em um televisor mais antigo. Sem contar que com essa nova dinâmica de TV digital pode-se ainda usufruir do uso de aparelhos celulares que dispõem desse tipo de integração com as novas televisões, permitindo assim o acesso ao conteúdo televisivo no próprio dispositivo, mantendo, desta forma, os mesmos benefícios do sinal digital.

Nos anos 1970, a revolução tecnológica possibilitou a propagação da TV a cabo e por satélite. O modelo se firmou na década seguinte, exigindo novas maneiras de regulação. O número de canais começou a aumentar significativamente, dissipando cada vez mais a audiência entre eles. Desta forma, a programação começou a ser mais segmentada, tendo como foco um menor público, contudo mais fidelizado ao canal (GALPERIN, 2003).

Em meados da década de 80, as ilhas de edição digitais [8]ofereciam mais flexibilidade e muito mais recursos aos editores da época. Considera-se essa evolução tecnológica como o nascimento da TV digital. Na perspectiva da recepção, a TV passou a contar com o controle remoto. Iniciaram-se assim os avanços necessários que demostravam ser possível também a

[7] Significado no Glossário.
[8] Ilhas de edição servem como editores de vídeos, sendo uma estação de edição não linear em alta definição e de alto desempenho. Fonte: (CAMPVIDEO, 2016).

transmissão digital, exaustivamente testada na década de 90, porém na internet, com cabos. Praticamente ao mesmo tempo, iniciaram-se os testes para a modulação do sinal audiovisual no quesito de transmissão terrestre e por satélite (MONTEZ; BECKER, 2005). Tivemos assim uma segmentação das diferentes gerações, conforme apresentado anteriormente no Quadro 1.

Toda essa evolução em termos físicos, tecnológicos, de equipamentos e infraestrutura deve ser acompanhada no decorrer dos anos na mesma proporção das iniciativas de planejamento estratégico que as corporações privadas exercem em seus negócios, porém, e sobretudo, com o acompanhamento do governo em relação aos investimentos em capacitações técnicas, de proficiências operacionais e de gestão do conhecimento dos cidadãos brasileiros, pois de nada adiantará termos progressos tecnológicos sem o mesmo nivelamento de aperfeiçoamento nos quesitos de mão de obra qualificada e conhecimento para tomadas de decisão, seja nas escolhas de consumo, seja nas decisões de negócio. Neste sentido, o Ministério de Ciência e Tecnologia do Governo Brasileiro, em seu chamado Livro Branco, revela:

> No mundo contemporâneo é limitado o espaço para improvisações. É possível ser ambicioso e é necessário estar preparado para aproveitar as oportunidades e usufruir os benefícios que a Ciência e Tecnologia podem propiciar. Para tanto, embora o País conte com experiências bem-sucedidas e um firme ponto de partida, é necessário fortalecer a capacidade de planejamento, prospecção e delineamento de visões estratégicas. Isso se faz mediante prospecção e planejamento consistentes; acompanhamento e avaliação; articulação de esforços públicos e privados; foco e diretrizes; incentivos e meios adequados; pessoas preparadas e empreendedoras; infra-estrutura e instituições qualificadas. A construção dessas competências requer tempo e esforços permanentes da sociedade. A criação do Centro de Gestão e Estudos Estratégicos (CGEE), em setembro de 2001, constitui-se um passo nesta direção (BRASIL, 2002).
>
> IV. Expandir e modernizar o sistema de formação de pessoal para Ciência, Tecnologia e Inovação:
>
> --> Colaborar com a implantação de novas diretrizes curriculares, indicando revisões periódicas com vistas a formar cientistas, engenheiros e demais profissionais com perfis adequados às novas exigências do Sistema Nacional de Ciência, Tecnologia e Inovação (BRASIL, 2002).

Fica claro que de fato não basta haver uma massificação numerosa de equipamentos sofisticados se não houver a formação das pessoas, promovendo uma cultura não somente de contato, disponibilização e acessibilidade, mas, sobretudo, de qualificação para que se conheça adequadamente essas novas gerações de equipamentos, cada vez mais domésticos, de inovação tecnológica.

2.1 A interatividade da TV digital

A interatividade, sem dúvida, é um dos apelos mais envolventes da TV digital, pois é possível, por exemplo, executar aplicativos no aparelho televisor. Por intermédio de tais aplicações, o telespectador pode ter acesso a uma série de serviços e entretenimentos, como comerciais, operações bancárias, enquetes, entre outros. Assim como os smartphones e celulares mais modernos se aproximaram do computador e da Internet, a interatividade faz o mesmo agora para a televisão. Nesse contexto, quanto maiores as possibilidades interativas, maior deverá ser o cuidado do usuário em relação àquilo que manipula, envia e descarta em termos de informação digital (som, imagem etc.), de modo que a proatividade pode cobrar seu preço se não houver uma orientação adequada condizente com as políticas de privacidade, que iremos abordar e melhor entender nos capítulos subsequentes deste trabalho.

Segundo José Moran (2002, p. 6), a interatividade está associada à bidirecionalidade do processo, em que o fluxo se dá em duas direções, ou seja, entre quem oferece a informação para proporcionar a interatividade e quem a recebe.

> Marshall McLuhan (1995) divide a interatividade presente na mídia em duas categorias que se distinguem entre si pelos efeitos que exercem sobre os usuários: o meio quente e o meio frio. A mídia quente fornece informação saturada, tolerando pouca ou nenhuma interação, a exemplo do rádio, cinema, fotografia e do alfabeto fonético. Já os meios frios geram conteúdos que podem ser completados. Eles incluem os usuários no processo de comunicação, tornando-os agentes participativos, promovendo o intercâmbio de informações. Pode-se mencionar como modelos o telefone, a televisão, os escritos hieroglíficos ou ideogrâmicos. Contextualizando a descrição de McLuhan, os meios frios estariam também relacionados aos novos media como a internet, consagrada pela bidirecionalidade. (PORTO; CIRNE, 2009).

Se usarmos o contexto com base na evolução tecnológica dessa mídia, podemos classificar a interatividade, de acordo com Lemos (1997), em sete níveis de interação (Quadro 2).

Quadro 2 – Níveis de interatividade da televisão

Nível	Descrição
0	A televisão expõe imagens em preto e branco e dispõe de um ou dois canais. A ação do espectador resume-se a ligar e desligar o aparelho, regular volume, brilho ou contraste e trocar de um canal para outro.
1	A televisão ganha cores, maior número de emissoras e controle remoto; o *zapping* vem anteceder a navegação contemporânea na *web*. Ele facilita o controle que o telespectador tem sobre o aparelho, prendendo-o ao mesmo tempo ainda mais à televisão.
2	Alguns equipamentos periféricos vêm se acoplar à televisão, como o vídeo cassete, as câmeras portáteis e os jogos eletrônicos. O telespectador ganha novas tecnologias para apropriar-se do objeto televisão, podendo agora também ver vídeos e jogar, gravar os programas veiculados e vê-los ou revê-los quando quiser.
3	Já aparecem sinais de interatividade de características digitais. O telespectador pode interferir no conteúdo utilizando o telefone (como no programa "Você Decide", da Rede Globo de Televisão), o fax ou o correio-eletrônico.
4	A televisão torna-se interativa, e o espectador pode participar do conteúdo por meio da rede telemática em tempo real, escolhendo ângulos de câmera, diferentes encaminhamentos das informações etc. Apesar dessa definição de Lemos (1997), no nível 4 o telespectador ainda não tem controle total sobre a programação. Ele apenas reage a impulsos e caminhos predefinidos pelo transmissor. Isso ainda não é TV interativa, pois contradiz a característica do "não-default", definida no estágio 4. A TV ainda é reativa, sendo necessários pelo menos mais três níveis de interatividade para torná-la proativa.
5	O telespectador pode ter uma presença mais efetiva no conteúdo, saindo da restrição de apenas escolher as opções definidas pelo transmissor. Passa a existir a opção de participar da programação enviando vídeo de baixa qualidade, que pode ser originado por intermédio de uma webcam ou de uma filmadora analógica. Para isso, torna-se necessário um canal de retorno ligando o telespectador à emissora, chamado de canal de interação.
6	A largura de banda do canal aumenta, oferecendo a possibilidade de envio de vídeo de alta qualidade semelhante ao transmitido pela emissora. Dessa forma, a interatividade chega a um nível muito superior à simples reatividade, como caracterizado no nível 4.
7	A interatividade plena é atingida. O telespectador passa a se confundir com o transmissor, podendo gerar conteúdo. Esse nível é semelhante ao que acontece na internet hoje, em que qualquer pessoa pode criar um site, bastando ter as ferramentas adequadas para tal. O telespectador pode produzir programas e enviá-los à emissora, rompendo o monopólio da produção e veiculação das tradicionais redes de televisão que conhecemos hoje.

Fonte: Lemos (1997).

Toda essa evolução da interatividade descrita anteriormente em diferentes fases ou níveis demonstra paralelamente toda uma evolução também da tradicional TV, que agora pode ser chamada de Smart TV.

É importante neste momento fazer uma pequena reflexão no que se refere às práticas culturais das tecnologias da informação e comunicação aos olhos da evolução digital e tecnológica. No nosso caso específico temos como foco a Smart TV. O progresso dos

recursos técnicos que esse equipamento sofreu no decorrer do tempo foi algo transformador para o processo de comunicação e experiência do usuário. O "espírito da coisa" continua o mesmo, ou seja, o telespectador continua a assistir aos canais de televisão por meio de uma grade televisiva de nosso país. Anteriormente, o esforço operacional, de manipulação-controle, e até mesmo intelectual do usuário, era mínimo, irrisório diante da TV. Mas o tempo passou e a TV tornou-se uma Smart TV. Importante agora pensar também no usuário, isto é, no smart-usuário. É preciso entender se ele está de fato preparado para a nova dinâmica que a Smart TV nos traz hoje. É importante que ele tenha preocupações preventivas com a configuração e, claro, com a segurança de suas informações.

Segundo a Nielsen (BRIGATTO, 2016), os proprietários de televisores conectados no Brasil são, em sua maioria, homens, casados, com idade entre 20 e 40 anos, com filhos e renda anual superior a R$ 47 mil. O principal fator para a compra é a possibilidade de ter acesso a uma maior variedade de conteúdo, especialmente vídeo. Dos usuários, 84% usam aplicativos para assistir a filmes e séries – na sequência estão os de rádio e música, com 54%. O horário em que mais se assiste a vídeos nesses serviços é entre 20h e 23h. Em média, os consumidores assistem a 3,3 horas desse tipo de conteúdo. "A TV voltou a ser o centro de entretenimento da casa das pessoas", disse Priscilla Giron, gerente de produtos da Samsung (BRASILEIROS..., 2015).

De uma maneira geral, essas chamadas "práticas culturais" com as quais o usuário-cliente se depara em sua Smart TV parecem não estar de fato no mesmo padrão-patamar de evolução que o próprio equipamento sofreu, com seus novos e inúmeros recursos de interação e integração. E subestimar isso, sobretudo no panorama da chamada Internet das Coisas que estamos vivenciando (algo que já se tornou inexorável), é, no mínimo, um risco plausível a se correr no que se refere à segurança das informações.

Deve ficar claro que a evolução do "equipamento televisão" é diferente da evolução da transmissão, que deixou de ser analógica e tornou-se digital. É notório que o fim dos "fantasmas" e ruídos foi um ganho considerável na qualidade de se assistir à TV. Deve-se ressaltar que a tecnologia da TV digital aparece como um progresso de fato em relação à TV analógica, possibilitando, assim, inúmeras novidades na maneira de se fazer e de se assistir à televisão.

2.2 Cultura x Smart TV

Com a chegada da Smart TV, não há dúvidas de que ficou mais interessante utilizá-la. Porém, esse "utilizar" ainda é fortemente percebido como utilização básica. É praticamente comprar muito para consumir pouco. Ou seja, existem, de fato, inúmeros recursos na Smart TV de hoje, contudo, pela cultura, pela desinformação ou até mesmo por "medo de mexer" nela, o usuário acaba ficando somente com o elementar "assistir à TV", literalmente. Ele deixa, por exemplo, de utilizar e explorar os recursos que uma Smart TV oferece, como jogar videogames, utilizar tocadores de *Blu-ray Disc*, streaming media set top boxes, TiVo[9] e alguns receptores de áudio/vídeo com recursos midiáticos interessantes, e de explorar toda uma interação on-line de áudio e vídeo.

Quando se fala somente em assistir à TV, um ponto deve ficar claro para não haver confusão. O cliente-usuário, consumidor da TV inteligente, atualmente, além de assistir habitualmente à TV por uma grade televisiva do canal a cabo ou das próprias emissoras nativas do país, tem o recurso de poder também estar on-line (na internet) em sua Smart TV buscando canais de programação alternativos, acessando programas já gravados ou mesmo ao vivo pela internet. O mais recente relatório destacado pela NPD *Connected Intelligence* revela que quase seis em cada dez consumidores que possuem uma HDTV conectada acessam serviços *Over-the-Top* (OTT)[10] de vídeo por meio do dispositivo (Figura 3).

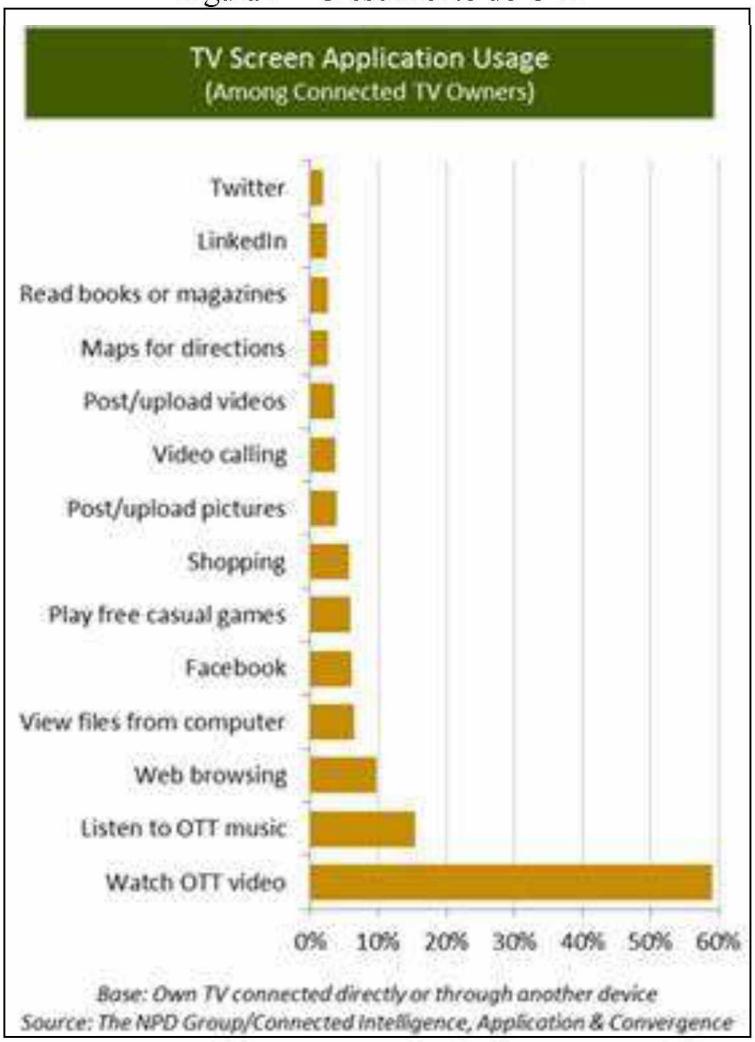
> Quando se trata de aplicativos, de acordo com o relatório Connected Application Intelligence, 40% das TVs conectadas à Internet, seja através da própria TV ou através de outro dispositivo, são usadas para assistir a filmes no Netflix. Quase um em cada cinco aparelhos conectados são usados para videos do YouTube (17%), e um em cada dez para assistir a vídeos no Hulu (11%). (RAPID TV, 2013).

---

[9] **TiVo** é uma marca popular de gravador de vídeo digital (*Digital Video Recorder* - DVR) que pode também ser chamado de gravador de vídeo pessoal (*Personal Video Recorder* - PVR).

[10] Na radiodifusão, OTT refere-se à entrega de áudio, vídeo e outras mídias por intermédio da Internet sem o envolvimento de um operador de sistema múltiplo no controle ou na distribuição do conteúdo. Os consumidores podem acessar o conteúdo OTT através da conexão à internet com dispositivos como computadores e portáteis, consoles de jogos (como o PlayStation 4, WiiU e Xbox One), set-top boxes (como o Roku), smartphones (incluindo Android phones, iPhones, e Windows phones), TV inteligentes (tais como Google TV) e demais genéricos.

Figura 3 – Crescimento do OTT



Fonte: NPD Group (2015).

Percebemos, assim, que a evolução existe, e que muito do que antes não poderíamos realizar numa televisão tradicional pode ser feito hoje com uma Smart TV; as possibilidades se multiplicam cada vez mais pelo simples fato de se estar on-line. Todavia, somos capazes de compreender também que quanto mais recursos e domínios, maior a responsabilidade e os cuidados que devemos ter em seu uso e acesso, pelo fato de que com a Smart TV estamos conectados à internet. O poder de usufruir das redes sociais, de canais multimídia com programas gratuitos e de todos os outros recursos citados anteriormente presentes nas Smart TVs faz com que o usuário esteja imerso num universo idêntico ao de um PC, de um notebook ou de um celular, devendo, portanto, se precaver de algumas ameaças (sobretudo por conseguir utilizar o recurso de DLNA, de que falamos na introdução deste trabalho) que serão abordadas mais detalhadamente no capítulo 4.

Com uma visão mais ampliada e estando mais atentos ao que se vislumbra em termos da evolução e do benefício que as Smart TVs podem trazer, esquecendo-nos do lado consumista de sua utilização e pensando no prazer de usufruir das melhores inovações tecnológicas possíveis de se obter, podemos constatar que as TVs inteligentes apresentam um outro lado: a retração do consumo das assinaturas de TV fechada (como NET, SKY, dentre outras), uma vez que se pode estar on-line, integrado à internet, com *widgets* que estabelecem recursos para assistir a documentários, filmes, shows, programas esportivos, dentre outros (por exemplo: Crackle, Netflix, NetMovies e SundayTV).

Por sua vez, é importante desmistificarmos um pouco esse processo consumista, classificatório e de certa forma ciclicamente social. Renato Dagnino (2004) refere-se a três tipos de conceitos: a Tecnologia Apropriada (TA), a Tecnologia Convencional (TC) e a Tecnologia Social (TS). Coloca-se neste prisma a entrada da Smart TV como uma TA e a televisão tradicional como uma TC, de maneira que depois de muito tempo começou-se a entender e a caracterizar a TA como "um conjunto de técnicas de produção que utiliza de maneira ótima os recursos disponíveis de certa sociedade, maximizando, assim, seu bem-estar (DAGNINO, 2004, p. 86).

> Por entenderem a ciência como uma incessante e interminável busca da verdade livre de valores e a tecnologia como tendo uma evolução linear e inexorável em busca da eficiência, os críticos da TA não podiam perceber seu significado. Em vez de entendê-la como o embrião de uma superação do pessimismo da Escola de Frankfurt e da miopia do marxismo oficial, eles a visualizavam como uma ridícula volta ao passado. (NOVAES; DAGNINO, 2004, p. 34).

Fica aqui uma reflexão: se as Smart TVs foram pensadas para uma classe com maior poder aquisitivo, pois são mais caras do que as tradicionais, podemos afirmar que o perigo da "insegurança das informações" e o não entendimento das políticas de privacidade e a aderência a elas fica somente a cargo dessa classe? É possível acreditar ainda que a classe "desfavorecida", não portadora de recursos financeiros suficientes para ter acesso a uma Smart TV, não se torna refém dessa falta de segurança das informações, não ficando à mercê da quebra de sua privacidade? Por outro lado, a classe com poder aquisitivo mais alto, e que possui uma ou mais Smart TVs (sem contar, é claro, as próprias empresas), deveria possuir um papel de maior responsabilidade social em relação à segurança das informações?

> Assim, entendida como um processo de inovação a ser levado a cabo, coletiva e participativamente, pelos atores interessados na construção daquele cenário desejável, a TS se aproxima de algo que se denominou, em outro contexto, "inovação social" (Dagnino e Gomes, 2000). O conceito de inovação social, entendido ali a partir do conceito de inovação – concebido como o conjunto de atividades que pode englobar desde a pesquisa e o desenvolvimento tecnológico até a introdução de novos métodos de gestão da força de trabalho, e que tem como objetivo a disponibilização por uma unidade produtiva de um novo bem ou serviço para a sociedade –, é hoje recorrente no meio acadêmico e cada vez mais presente no ambiente de Policy Making. Esse conceito engloba, portanto, desde o desenvolvimento de uma máquina (hardware) até um sistema de processamento de informação (software) ou de uma tecnologia de gestão – organização ou governo – de instituições públicas e privadas (orgware) (DAGNINO, 2004).

O conceito de inovação social é usado por Dagnino e Gomes (2000) para destacar a referência ao conhecimento – que de certa forma é intangível ou incorporado às pessoas ou equipamentos, sendo tácito ou codificado –, tendo como foco principal o aumento da efetividade dos processos, bem como dos serviços e produtos vinculados à satisfação não tecnológica. Não querendo excluir o anterior, associa-se a um distinto código de valores, com formas e estilo de desenvolvimento, funcionando como um "projeto nacional" com objetivos de cunho social, político, econômico e ambiental. O conceito de inovação social engloba três tipos de inovação: hardware, software e orgware (DAGNINO; GOMES, 2000).

É necessário que, hoje, o fabricante de Smart TV se concentre menos em revolucionar o que será entregue como novidade e mais na simplificação da experiência do usuário e, claro, na segurança de suas informações. Sobretudo que agora, mais do que nunca, há a tendência de maior integração com redes sociais, eletroeletrônicos e eletrodomésticos e toda uma centralização de vídeo-multimídia, com inúmeros recursos de aplicativos para videogame que interagem com a Smart TV, além ainda da possibilidade de busca de conteúdo, dos próprios dispositivos mobile e dos diversos tipos de sinais de comunicação e transmissão que aumentam consequentemente o leque de novas brechas e vulnerabilidades.

2.3 Importância das políticas de privacidade para a segurança das informações

Uma política de privacidade, além de possuir um cunho orientativo, deve funcionar como um instrumento legal do fabricante direcionado para o cliente, e sobretudo como um mecanismo de comunicação que não somente informa, mas ajuda o usuário a entender quais de seus dados poderão ser absorvidos durante sua utilização da Smart TV. Ela deve permitir a ele ter o livre arbítrio de, em alguns casos, ativar ou desativar os recursos de envio/captação

de informações para o fabricante. Desta forma, podemos melhor entender a frase "toda atividade comunicativa é uma atividade educativa, e vice-versa" (FORTUNATO, 2010, [p. 2]).

Pelos resultados da pesquisa talvez possamos perceber que o próprio cliente-usuário terá que se autoeducar no processo de compreender o que é uma política de privacidade, sua importância pelo que ela traz de informação e sua relação com relação à segurança das informações. Pode acontecer até de o fabricante não ter muito interesse em fortalecer ou garantir tal entendimento, mas sua política precisa estar publicada em algum lugar. A política de privacidade seria o conteúdo ou o "dever de casa" a ser aprendido/assimilado pelo cliente-usuário, que deveria ter a atitude de concretizar esse processo de se autoeducar, uma vez que a autonomia de reivindicar as políticas de privacidade criadas pelo fabricante o cliente-usuário possui, mesmo que o primeiro de certa forma possa não querer que o segundo tenha essa "liberdade intelectual".

2.4 As políticas de privacidade e a IoT

Temos presenciado nos últimos tempos uma grande repercussão relacionada aos cuidados com a segurança das informações no contexto da Internet das Coisas (IoT). Com toda a integração e interação dos diversos eletrodomésticos e demais recursos de uso cotidiano em nossas casas e empresas, e com uma acessibilidade cada vez maior possibilitada pelos aparelhos móveis, percebemos o quanto estamos cada vez mais on-line, com diversos aparelhos sincronizados e dinâmicos.

Estamos cada vez mais inseridos num ambiente que necessita de conectividade disponível, eficiente e confiável. Estando, assim, constantemente conectados, devemos procurar saber se possuímos algum tipo de segurança na transição da gama infinita de informações que fazemos trafegar na rede de um equipamento para outro, pois, muitas das vezes, pelo simples fato de estarmos on-line automaticamente e sem nos darmos conta disso, podem ocorrer inúmeras transmissões de dados sem que consintamos ou tenhamos conhecimento prévio do que está sendo absorvido, captado, compartilhado.

Neste contexto, possuir e conhecer as políticas de privacidade dos equipamentos que estão nesse ambiente em que estamos envolvidos é extremamente importante, sobretudo no quesito referente ao respaldo legal e jurídico dos direitos de uso e transmissão da informação gerada, manipulada pelo fabricante, no caso de nosso estudo-assunto, de uma Smart TV.

Claro que a IoT engloba muitos outros tipos de equipamentos, além das televisões, mas sendo a Smart TV uma evolução de um recurso de comunicação de massa (a tradicional TV) muito utilizado e encontrado normalmente em grande parte das empresas e casas, temos que levar em consideração o cuidado de saber exatamente o que consta nas políticas de privacidade de cada fabricante, uma vez que há a tendência de que toda TV venha a ser uma Smart e que seu preço de venda caia, tornando-a cada dia mais acessível às diversas classes sociais.

> No atual cenário de retração no mercado, são as chamadas Smart TVs que passaram a atrair o interesse do brasileiro. Levando em conta todos os televisores de tela fina, foram vendidas, no primeiro trimestre de 2016, em comparação com igual período de 2015, 28% unidades a menos, conforme dados da consultoria GfK. Mas no segmento das TVs com acesso à internet houve aumento de 6,4%. Hoje, as Smart TVs já correspondem a 50% das vendas no país. Em meados do ano passado, rondavam os 39%. Em 2014, os 22%. (FABRICANTES..., 2016).

No Quadro 3, após leitura e estudo das informações contidas na política de privacidade de alguns dos principais fabricantes, conforme pesquisa realizada pela LCD TV Buying Guide's (LCD-TV, 2017), e consultas em diversos outros sites e associações, foi traçado um panorama geral daquilo que os 12 principais fabricantes revelam em relação à privacidade das informações do usuário-cliente (quando se tem[11]).

Para os consumidores/usuários que acreditam que a privacidade é importante, vale destacar algumas questões, apontadas a seguir, que poderão ser respondidas por meio dos resultados consolidados no Quadro 3:

- Quem recolhe as informações pessoais?
- Quais tipos de dados são armazenados (por exemplo, hábitos de visualização ou pesquisas importadas)?
- Qual é o propósito de armazenamento desses dados?
- Com quem se compartilham tais dados?[12]

Conforme relatório de pesquisadores holandeses (SCHERMER; FALOT, 2014), todos os fabricantes de Smart TV monitoram o que os usuários assistem e quais são seus interesses, uma vez que estes dão aos fabricantes de TV permissão para coletar e usar seus dados a partir

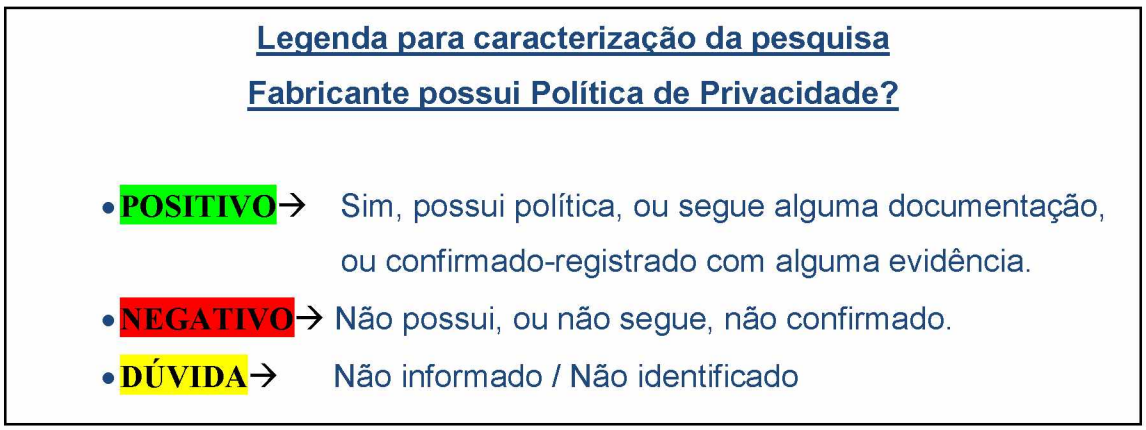
[11] Quando se tem, pois nem todos estes 12 principais fabricantes listados no quadro 3, publicam claramente sua política de privacidade. E claro que existem outros fabricantes, que aqui não foram relacionados, como por exemplo: Mitsubishi, RCA, Hitachi, JVC, AOC,CCE, dentre outras.

[12] Os critérios foram avaliados com base nas políticas de privacidade encontradas de cada fabricante.

do momento em que aceitam os termos de privacidade propostos pela empresa. O relatório destaca ainda que todas as Smart TVs apresentam as práticas/os termos de privacidade ao instalar a TV.

Os usuários das Tvs inteligentes, podem, portanto, concluir que aceitar as condições de privacidade seja obrigatoriamente necessário, mas não é. Ou seja, consegue-se utilizar regularmente uma Smart TV, mesmo depois de serem rejeitados os termos de privacidade do fabricante. Ela só não opera todas as funções inteligentes, ou apenas parcialmente. A grande questão é que eles surgem de novo magicamente na tela se o usuário estiver on-line (na internet) ou tentar utilizar algum outro recurso inteligente da Smart TV. Sendo assim, em razão de tanta insistência ou incômodo, o usuário acaba por concordar com tais termos.

Figura 4 – Política de Privacidade x Fabricante de Smart-TV



Fonte: Pesquisa/Elaboração do próprio autor.

Observação[13]: Percebe-se que o primeiro critério é justamente saber se determinado fabricante, possui ou não uma política de privacidade. Daí em diante, os critérios são co-dependentes da política de privacidade, havendo consequentemente uma relação direta.

[13] Quadro 3 elaborado em: 17/06/2016.
As políticas de privacidade aqui coletadas não representam modelos/series específicos de determinado fabricante. Os que constam como 'POSITIVO" em termos de possuir uma política de privacidade oficial, representa como documento geral para suas Smart-Tv's, por não especificarem modelos/series distintas.
Para visualização em formato InfoGraph:
http://media.wix.com/ugd/fdef72_2382810fc7dc41e7ac5c501da6139109.pdf

Quadro 3 - Comparação das características de privacidade por fabricante

CRITÉRIO / Fabricante	SAMSUNG	LG	PHILIPS TPVISION	SONY	Panasonic	VIZIO	XIAOMI	Hisense	TCL	SHARP	TOSHIBA	PHILCO
Possui política de privacidade para a Smart TV?	**POSITIVO** http://www.samsung.com/sg/info/privacy/smarttv.html	**POSITIVO** http://gb.lgappstv.com/appspc/footer/footer/moveDeviceTerms.lge?type=S_PRG&level=2&link=202	**POSITIVO** http://www.tpvision.com/wp-content/uploads/SMARTTVPrivacyandCookiePolicy1May2014.pdf	**NEGATIVO** Possui, porém somente as são genéricas divulgadas, como apresentado abaixo. Para Smart-TV especificamente, só na própria TV. https://www.sony.co.in/section/privacypolicy http://www.sony.co.uk/support/en/article/66466 http://www.sonymax.tv/en-us/privacy-policy http://www.sonypictures.com/corp/privacy.html https://account.sonyentertainmentnetwork.com/info/privacy-policy.action https://products.sel.sony.com/SEL/legal/privacy.html	**NEGATIVO** Possui,porém somente as genéricas são divulgadas, como apresentado abaixo. http://www.panasonic.com/br/privacy-policy.html http://www.panasonic.com/global/privacy-policy.html http://www.panasonic.aero/PrivacyPolicy.aspx	**Positivo** http://www.vizio.com/privacy	**NEGATIVO** Possui, porém somente as genéricas são divulgadas, como apresentado abaixo http://www.mi.com/sg/about/privacy/ http://www.mi.com/en/privacy/	**NEGATIVO** Possui, porém somente as genéricas são divulgadas, como apresentado abaixo. http://www.hisense-usa.com/contact/privacy.asp http://hisense.co.uk/pages/privacy	**NEGATIVO** Possui, porém somente as genéricas são divulgadas, como apresentado abaixo http://www.tclusa.com/termsprivacy/ http://www.tclchinesetheatres.com/privacy-policy/ http://www.tclgrp.co.uk/privacy-policy/ http://tclmedia.com.au/privacy-policy/	**POSITIVO** http://www.sharpusa.com/SmartCentral/privacypolicy.aspx	**NEGATIVO** Possui, porém somente as genéricas são divulgadas, como apresentado abaixo http://www.toshibamea.com/en/privacy-policy https://www.toshiba.eu/innovation/generic/PRIVACY_POLICY/ http://toshiba.com.my/privacy_policy/ https://www.toshibatec.co.jp/en/privacy/ https://www.toshiba-india.com/cricketseries/privacy-policy http://us.toshiba.com/website/privacy-policy	**DÚVIDA** Inexistência de políticas de privacidade. O que se encontrou foi no máximo políticas de privacidade referente aos sites da phico.

Afirma que coleta, usa, compartilha e armazena informações por meio da Smart TV?	**POSITIVO**	**POSITIVO**	**POSITIVO** Por meio do "Social TV", no âmbito das redes sociais.	**NEGATIVO**	**NEGATIVO**	**POSITIVO**	**NEGATIVO**	**NEGATIVO**	**NEGATIVO**	**POSITIVO** Por meio do Smart-Center	**NEGATIVO**	**DÚVIDA**
Determina qual conteúdo estará disponível para o usuário com base no código postal cadastrado (CEP)?[14]	**POSITIVO**	**POSITIVO**	**POSITIVO** Utiliza o recurso chamado "Akamai", com base em seus servidores http://www.akamai.com	**NEGATIVO**	**NEGATIVO**	**POSITIVO**	**NEGATIVO**	**NEGATIVO**	**NEGATIVO**	**POSITIVO**	**NEGATIVO**	**DÚVIDA**
Coleta informações sobre o conteúdo que o usuário assistiu, comprou, "baixou" ou transmitiu por meio de aplicações da Smart TV?	**POSITIVO**	**POSITIVO**	**POSITIVO**	**NEGATIVO**	**NEGATIVO**	**POSITIVO**	**NEGATIVO**	**NEGATIVO**	**NEGATIVO**	**POSITIVO**	**NEGATIVO**	**DÚVIDA**
Coleta informações sobre aplicativos acessados por meio dos painéis?	**POSITIVO**	**POSITIVO**	**POSITIVO**	**NEGATIVO**	**NEGATIVO**	**POSITIVO**	**NEGATIVO**	**NEGATIVO**	**NEGATIVO**	**POSITIVO**	**NEGATIVO**	**DÚVIDA**
Coleta informações sobre os cliques no "like", "dislike", "assista agora" ou outros botões da Smart TV?	**POSITIVO**	**POSITIVO**	**POSITIVO**	**NEGATIVO**	**NEGATIVO**	**NEGATIVO**	**NEGATIVO**	**NEGATIVO**	**NEGATIVO**	**NEGATIVO**	**NEGATIVO**	**DÚVIDA**

[14] O CEP é utilizado para alguns serviços on-line, como notícias, clima e guia de programação. Exemplo: http://www.samsung.com/br/support/model/UN55H6300AGXZD.

Coleta informações sobre os termos da consulta que o usuário faz quanto aos recursos de pesquisa da Smart TV, incluindo a procura por determinado conteúdo de vídeo?	POSITIVO	POSITIVO	DÚVIDA	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	DÚVIDA
Coleta informações do dispositivo, como o endereço IP, informações armazenadas em cookies e tecnologias similares, informações que identificam o hardware ou o software de configuração, informações do navegador e a(s) página(s) acessada(s) pelo usuário?	POSITIVO	POSITIVO	POSITIVO	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	DÚVIDA
Refere-se à possibilidade de ativar/desativar a coleta de informações sobre fluxos de vídeo vistos na Smart TV?	POSITIVO	DÚVIDA Somentedurante o registro	DÚVIDA Somentedurante o registro	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	DÚVIDA
Há recomendações personalizadas e/ou propagandas e anúncios (espécie de ADS-PROVIDER)?	POSITIVO	POSITIVO	POSITIVO	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	DÚVIDA

Com base em recursos de sincronização automática e marketing interativo da Smart TV, existe a possibilidade de repasse de informações a terceiros (outros fornecedores), como IP e demais identificadores do dispositivo?	POSITIVO	POSITIVO Quando se usa o LivePlus	DÚVIDA	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	DÚVIDA
Existe a possibilidade da coleta de dados de reconhecimento de voz (podendo esta ser ativada/desativada)?	POSITIVO	POSITIVO	POSITIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	DÚVIDA
Há o registro das informações sobre quando e como o usuário utiliza os controles de gestos?	POSITIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	DÚVIDA
Há transmissão de reconhecimento facial?	DÚVIDA	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	DÚVIDA
Coleta informações sobre quando e como o recurso de reconhecimento facial é utilizado?	POSITIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	DÚVIDA
Há informações sobre o dispositivo, ou seja, sobre a Smart TV em si e seus agregados (ex: set-top box, controle remoto, leitor de DVD ou Blu-ray)?	NEGATIVO	POSITIVO	NEGATIVO	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	DÚVIDA

Há informações para autenticar a Smart TV com os servidores do fabricante, como o código do país e/ou o código postal da região, endereço IP, tipo de dispositivo (por exemplo, set-top box, DVD player etc.), endereço MAC, software e versão da plataforma, idioma, fabricante set-top box, resolução de tela e o número do modelo da Smart TV?	NEGATIVO	POSITIVO	POSITIVO Com base no "Device-ID".	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	DÚVIDA
Com base nos serviços vinculados para associados do fabricante, pode haver o compartilhamento das informações cadastrais do usuário da Smart TV com terceiros?	NEGATIVO	POSITIVO	POSITIVO	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	DÚVIDA
Há a possibilidade de utilização de alguma informação a fim de cumprir com processos legais ou de direito, sobretudo quando relacionada a procedimentos de compra on-line feitas pelo consumidor?	NEGATIVO	POSITIVO	POSITIVO	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	DÚVIDA

Refere-se ao poder de utilizar o processamento de dados do usuário em qualquer jurisdição/país, uma vez que ele concorda com a política de privacidade em questão?	NEGATIVO	POSITIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	DÚVIDA
Utiliza cookies e beacons[15] para repasse aos fornecedores/terceiros conveniados com o fabricante?	NEGATIVO	POSITIVO	POSITIVO	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	DÚVIDA
Garante que as comunicações entre o usuário da Smart TV e os servidores do fabricante estarão livres de acesso não autorizado por terceiros ou que o cliente não estará sujeito a violações de segurança?	NEGATIVO	DÚVIDA	POSITIVO	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	NEGATIVO	NEGATIVO	DÚVIDA	NEGATIVO	DÚVIDA
Existe a utilização de informações sobre DLNA?	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	DÚVIDA
No manual do usuário está anexada a política de privacidade ou ao menos há uma referência a esta?	DÚVIDA Referência somente ao uso do Skype. http://downloadcenter.samsung.com/content/UM/201204/20120405165133112/2012_Skype_Eng-0316-1.pdf	NEGATIVO http://www.lg.com/ca_en/products/documents/LS5700_Series_Spec_Sheet_ENG%20Final.pdf	DÚVIDA Referência somente ao uso do Skype. http://img.americanas.com.br/produtos/01/02/manual/119797176.pdf	NEGATIVO	NEGATIVO	POSITIVO [Página 20, item 6] http://cdn.vizio.com/documents/downloads/hdtv/E601iA3/UM_E601iA3.pdf	NEGATIVO	NEGATIVO	NEGATIVO	DÚVIDA	NEGATIVO	DÚVIDA

[15] *Beacons* são aparelhos de proximidade que emitem informações por meio da tecnologia *bluetooth*.

Apresenta glossário?	NEGATIV	NEGATIV	POSITIVO	NEGATIVO	NEGATIVO	NEGATI	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	DÚVIDA
Há uma explicação clara sobre o que será feito com os dados coletados?	NEGATIVO	POSITIVO	POSITIVO	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	DÚVIDA
Há a possibilidade de limpar/zerar todos os cookies e registros de navegação, bem como os registros do dispositivo?	NEGATIVO	NEGATIVO	POSITIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	NEGATIVO	DÚVIDA

Fonte: Elaborado pelo autor

Os resultados do Quadro 3 ilustram as características e a política de privacidade de cada empresa, mas, por mais que tenhamos observado em alguns itens "*não informado/não identificado*", a probabilidade de que alguns fabricantes possam fazer/executar os critérios, assim como outros que responderam "*sim*", pode ser grande, mesmo que isto não esteja formalizado em sua política, pelo fato não somente de as características das diversas Smart TVs no mercado serem muito similares, mas, sobretudo, em razão dos interesses dos fabricantes serem muito parecidos quando se fala em "querer entender o cliente" ou, de certa forma, em "investigar seus costumes e hábitos". Em alguns outros casos, de fato, pode ser que não exista determinado recurso.

Acreditamos que o pior posicionamento é o "não informado/não identificado", pois a omissão é mais grave do que negar aquilo que de fato não se consegue fornecer, prever, proteger ou garantir. Concordando com a política de privacidade, o usuário saberá que algo será executado ou não, e que a privacidade de suas informações pode estar em jogo.

Com a existência de textos longos e completamente obscuros, que dificultam uma leitura clara e imediata dos termos de privacidade, as chances de os usuários clicarem diretamente no "ok", "concordo", "li e aceito" para se livrar da incômoda e desgastante leitura é muito grande. Existem ainda alguns casos em que, mesmo havendo uma política de privacidade razoável e coerente para leitura, o fabricante praticamente "força" o usuário a clicar em "aceito/concordo" para poder ter condições de realizar as atualizações da conta ou de algum recurso inteligente da TV.

Outro ponto polêmico que vale destacar é que fica a impressão de que os fabricantes de Smart TV não cumprem com suas obrigações legais. Acreditamos que eles deveriam ser legalmente obrigados a informar aos consumidores-usuários sobre determinadas vantagens na coleta de informações destacadas no Quadro 3. Deveriam ainda solicitar de maneira independente, e não amarrada aos recursos a serem utilizados, o consentimento do usuário para a utilização de alguns dados, e também possibilitar o direito a este de acessar tais dados quando bem quiser (já que são seus), assim como de retirar seu consentimento de uso. Enfim, parece claro que os fabricantes de Smart TV, em diferentes situações, não respeitam o Marco Civil da Internet – Lei 12.965 fornecendo informação de forma clara, precisa, objetiva e de real interesse para o cliente-usuário.

Numa avaliação geral, observou-se o seguinte:

a) Samsung, LG, Phillips e Vizio são as que mais se preocupam em possuir uma política de privacidade e demais explicações neste contexto, divulgando-as com mais clareza e com fácil acesso ao público.

b) Sony e Panasonic possuem uma política de privacidade para a Smart TV, porém esta não é divulgada, e o público não tem acesso a ela. Ela é internamente visível apenas na própria televisão (ou seja, somente depois de adquirir o aparelho o usuário toma contato com ela). Há apenas políticas genéricas para um universo geral de eletroeletrônicos das fabricantes.

c) Samsung, LG e Phillips são as que mais possuem evidências de vulnerabilidades de segurança da informação (acreditamos que por serem as mais vendidas e visadas do mercado), o que será melhor analisado no próximo capítulo.

d) em termos do envio das informações **cadastrais-pessoais**, estas só serão coletadas e enviadas caso o usuário tenha realizado o registro de cadastro no *site* ou feito algum tipo de preenchimento de dados na própria Smart TV, que contém tais informações para efeito de suporte e facilidades no processo de garantia e fidelização (exemplos: Club Phillips, LG Store, LivePlus etc.).

e) todos os fabricantes de televisão utilizam a internet para acompanhar o que o usuário faz com sua Smart TV e quais são seus interesses. Isso significa, em termos de privacidade, ter acesso legal aos dados pessoais do usuário e poder utilizar tais informações da maneira que considerarem mais pertinente. Os fabricantes descrevem suas políticas literalmente escondendo seus propósitos com a utilização de jargões jurídicos, com textos prolixos e muitas vezes longos e cansativos.

f) é fato que existe uma impertinência muito grande por parte dos fabricantes em insistir (enquanto se está *on-line* – na internet) no surgimento de telas de apresentação de sua política de privacidade (quando esta ainda não foi aceita) para que assim, "forçadamente", o usuário a aceite e consequentemente possa usufruir mais dos recursos inteligentes da sua TV, porém tornando-se suscetível à coleta de suas informações pessoais. Para que essas telas não apareçam a todo o momento o usuário terá que tirar o cabo de rede ou não estar ligado ao Wi-Fi para a conexão da internet, ou seja, precisará ficar literalmente off-line. Alguns fabricantes adotam um outro método para reduzir a coleta de dados, ajustando as opções de privacidade da TV por meio dos menus do dispositivo (SCHERMER; FALOT, 2014).

g) LG Electronics: o LG TV configura os dados sobre o comportamento do espectador (forward) em *on* e *off* em termos de "publicidade personalizada" por meio do menu Geral, em Sobre o chamado Contrato de Usuário da TV.

h) Panasonic: não apresenta nenhum menu de privacidade, devendo o usuário redefinir a TV nas Configurações de Fábrica para rejeitar a Política de Privacidade do fabricante.

i) Philips: o usuário pode definir em Recomendações Pessoais *on* e *off*, selecionando no ícone da *App Gallery* as opções de botão no próprio controle remoto.

j) Samsung: o cliente pode escolher no menu Condições da Política retirar a permissão de transmitir seus hábitos de visualização.

k) Sony: o usuário pode alternar entre o "não concordo" e o acompanhamento de seus hábitos de visualização por meio da Ajuda no uso da TV e da informação de estatística de Suporte ao Cliente.

Seguem abaixo as características das políticas de privacidade de alguns dos principais fornecedores de Smart TV, bem como os riscos a que o usuário está sujeito quando abre mão de certos recursos.

Quadro 4 – As políticas de privacidade das Smart TVs e os riscos a que o usuário está exposto

Características	**Riscos**
Afirma-se que são coletadas, utilizadas, compartilhadas e armazenadas informações por meio da Smart-TV	As informações cadastrais do usuário podem ser utilizadas por outros fornecedores
Determina-se qual conteúdo estará disponível para o usuário com base no código postal cadastrado (CEP)	É possível identificar geograficamente onde o usuário se encontra
Coleta de informações sobre o conteúdo assistido, comprado, baixado ou transmitido pelo usuário por intermédio das aplicações da Smart TV	Identificação dos gostos e do perfil do usuário tendo por base o que ele que consome, o que pode ser utilizado para outros fins, servindo para descobrir seus interesses por intermédio de ligações, cartas ou e-mails falsos
Coleta de informações sobre aplicativos acessados nos painéis	Aumento da probabilidade de os principais aplicativos acessados/utilizados pelo usuário serem alvo de infecção por algum tipo de *malware* ou aplicativo malicioso

Coleta de informações sobre os cliques do usuário no "like", "dislike", "assista agora" e outros botões da Smart TV	Identificação dos gostos e perfil do usuário tendo por base o que ele consome, o que pode ser utilizado para outros fins, como descobrir interesses conhecidos por intermédio de ligações, cartas ou e-mails falsos
Coleta sobre os termos da consulta utilizados pelo usuário ao entrar nos recursos de pesquisa da Smart TV, incluindo a procura por determinado conteúdo de vídeo	Identificação dos gostos e perfil do usuário tendo por base o que ele consome, o que pode ser utilizado para outros fins, como descobrir interesses conhecidos por intermédio de ligações, cartas ou e-mails falsos. Possibilidade de indução ao apresentar resultados preestabelecidos conforme a base de dados acumulada no perfil de pesquisa do usuário, limitando novas possibilidades
Coleta de informações por meio do dispositivo, como o endereço IP, informações armazenadas em cookies e tecnologias similares que identificam o hardware ou o software de configuração, informações do navegador e páginas acessadas pelo usuário	Uma vez que o IP e demais informações foram coletadas ao trafegarem pela rede, o usuário pode estar suscetível à captura de dados para futuros ataques no âmbito da interceptação, alteração ou visualização de informações
Com base em recursos de sincronização automática e marketing interativo da Smart TV, existe a possibilidade de repasse de informações a terceiros (outros fornecedores), como IP e demais identificadores do dispositivo	Uma vez que o IP e demais informações foram coletadas ao trafegarem pela rede, o usuário pode estar suscetível à captura de dados para futuros ataques no âmbito da interceptação, alteração ou visualização de informações
Surgimento de recomendações personalizadas e/ou propagandas e anúncios (espécies de ADS-PROVIDER)	Permite a adwares carregarem outros programas internamente embutidos, causando algum tipo de oscilação normal da funcionalidade operacional do midlware e, mesmo que nem sempre seja um malware, causando maior sobrecarga de processamento
Possibilidade da coleta de dados de reconhecimento de voz (que podem ser ativados/desativados)	O que foi captado em termos de dados e de voz pode ser utilizado por fontes não confiáveis pelos canais que trafegam nas estruturas NGN (Next Generation Networks - Próxima Geração de Redes)
Possibilidade da coleta de informações para autenticar a Smart TV com os servidores do fabricante, como o código do país e/ou código	Identificação do nome do usuário e senha de acesso no processo de autenticação, que podem ser utilizadas para outros fins, como para comprar e

postal da região, endereço IP, tipo de dispositivo (por exemplo, set-top box, DVD player etc.), endereço MAC, software e versão da plataforma, idioma, fabricante set-top box, resolução de tela e número do modelo da Smart TV	adquirir novos produtos ou serviços em nome do cliente. Possibilidade de descobrir ainda os perfis de acesso a determinados recursos que os usuários possuem ou contrataram em termos de autorização, ferindo assim os princípios fundamentais da segurança das informações, podendo-se descobrir quem é, como acessa e o que acessa cada usuário.
Utilização das informações sobre DLNA	Possibilidade de identificar quais dispositivos/recursos estão integrados à Smart TV e demais informações

Fonte: Elaborado pelo autor

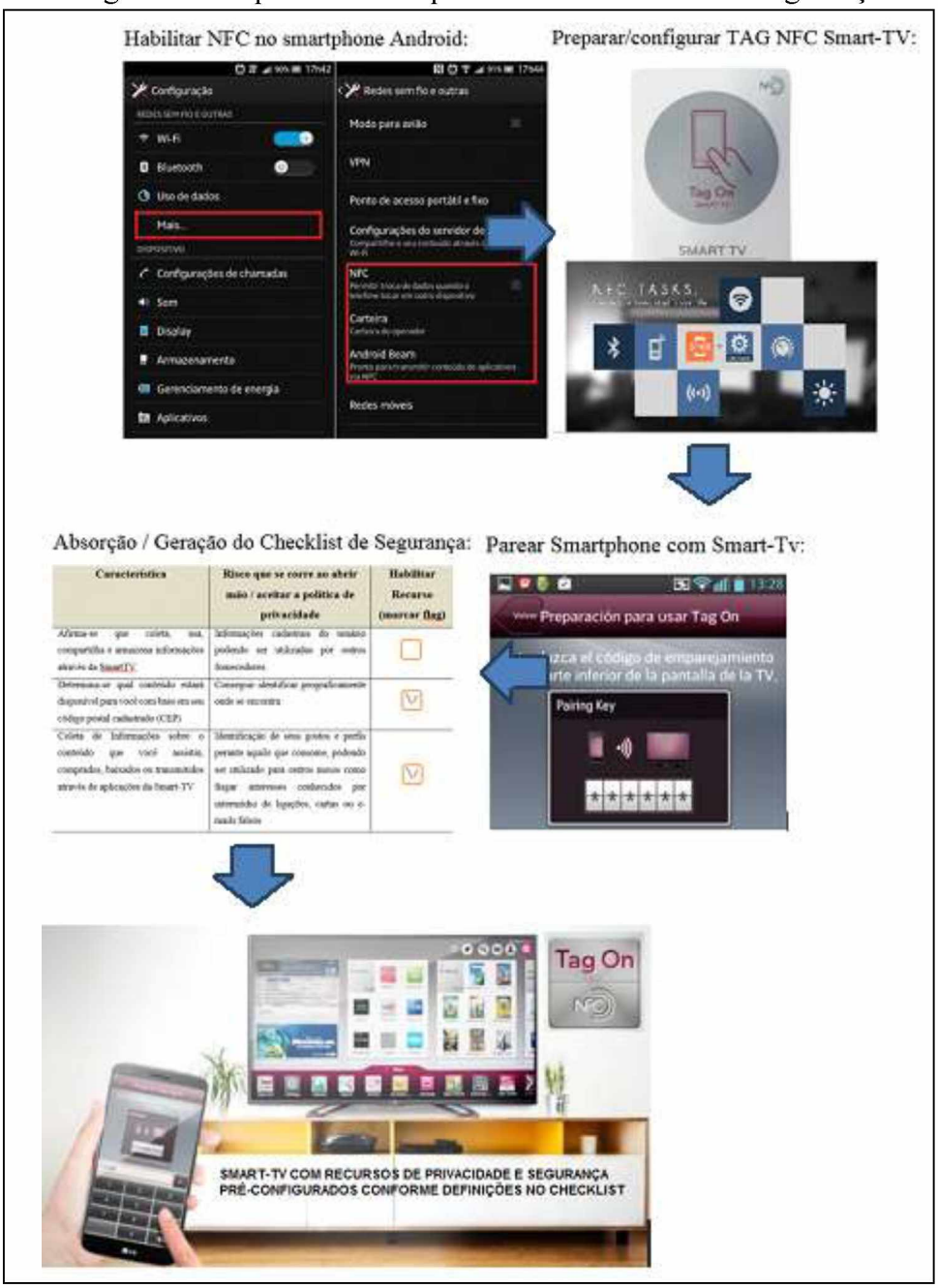
Acreditamos que uma ideia extremamente interessante a ser aplicada na prática após o desenvolvimento do projeto (como um trabalho futuro) seria a implantação da tecnologia NFC[16] (um exemplo é o LG TV Tag On para Smart TV e o Android Beam para celulares Android). A proposta se baseia em poder usufruir dos recursos de leitura aproximada do aparelho de smartphone em uma Smart TV (que teria que ser implantado de fábrica). Esta é uma tecnologia de comunicação de curto alcance e alta frequência, que permite a troca de dados com o equipamento eletrônico localizado dentro de uma área de 10 centímetros (3,9 polegadas) sem entrar em contato com ele. A tecnologia por trás da NFC permite que um dispositivo, conhecido como leitor, interrogador ou dispositivo ativo possa criar uma corrente de radiofrequência e assim se comunicar com outro dispositivo compatível NFC ou uma pequena tag NFC que detém a informação que o leitor deseja para dispositivos passivos.

Por possibilitar a comunicação bidirecional, a NFC é ideal para estabelecer conexões com outras tecnologias em razão de sua simplicidade de comunicação. Como a proposta deste trabalho é oferecer um aplicativo mobile que auxilie educacionalmente a fomentar uma maior e melhor cultura sobre as políticas de privacidade e segurança da informação, nada mais coerente que oferecer uma relação dos riscos que se corre ao aceitar a política de privacidade do fabricante (como demonstrado na tabela acima). Por intermédio da tecnologia NFC haveria a possibilidade da comunicação ativa (Smartphone <> Smart TV e Smart TV <> Smartphone). No aplicativo proposto neste trabalho ele executaria uma checklist com as

[16] *Near Field Communication*, abreviado como NFC, é uma forma de comunicação sem contato entre dispositivos como smartphones ou tablets. Essa comunicação permite que um usuário possa acessar com o smartphone mais de um dispositivo compatível com NFC para enviar informações sem a necessidade de tocar nos dispositivos ou de passar por várias etapas de configuração para estabelecer uma conexão. Trata-se de uma tecnologia rápida e conveniente. O NFC é popular em partes da Europa e da Ásia, e está rapidamente se espalhando pelos Estados Unidos (NFC, 2016).

informações específicas fornecidas por determinado fabricante de Smart TV, de maneira que o usuário marcaria nos *flags* disponíveis o que foi absorvido dos recursos de configuração referentes à privacidade e à segurança das informações. Tal recurso já estaria pré-configurado quando o usuário utilizasse o comando ou clicasse no botão para atualização. Segue um esboço dessa ideia na figura abaixo:

Figura 5 – Preparando NFC para executar checklist de segurança



Fonte: Elaborado pelo autor

Pesquisadores holandeses realizaram alguns testes de entendimento interpretativo para compreender a política de privacidade de alguns dos principais fabricantes de Smart TV (SCHERMER; FALOT, 2014), cujo resultado está exposto no quadro abaixo.

Quadro 5 – Resumo dos resultados

		LG	PANASONIC	PHILLIPS	SAMSUNG	SONY
FORMA	Facilidade de encontrar	++	+/-	-	-	+/-
	Acessibilidade	-	-	-	--	+
	Legibilidade	-	+/-	+	+	+
CONTEÚDO	Identificação*	+/-	-	++	++	-
	Propósito dos dados*	-	+/-	++	+/-	+
	Compartilhamento de informação com terceiros*	+/-	+	--	+	Nenhuma indicação
	Necessidade dos dados*	+/-	-	+/-	+/-	+
	Direitos do consumidor*	--	--	--	+/-	--
	Períodos de retenção	+/-	+/-	+	+/-	--
	Precauções de segurança	--	+/-	--	-	--
	Considerações de uso	-	-	+/-	-	-
PERMISSÃO	Permissão*	+/-	+/-	++	+/-	++

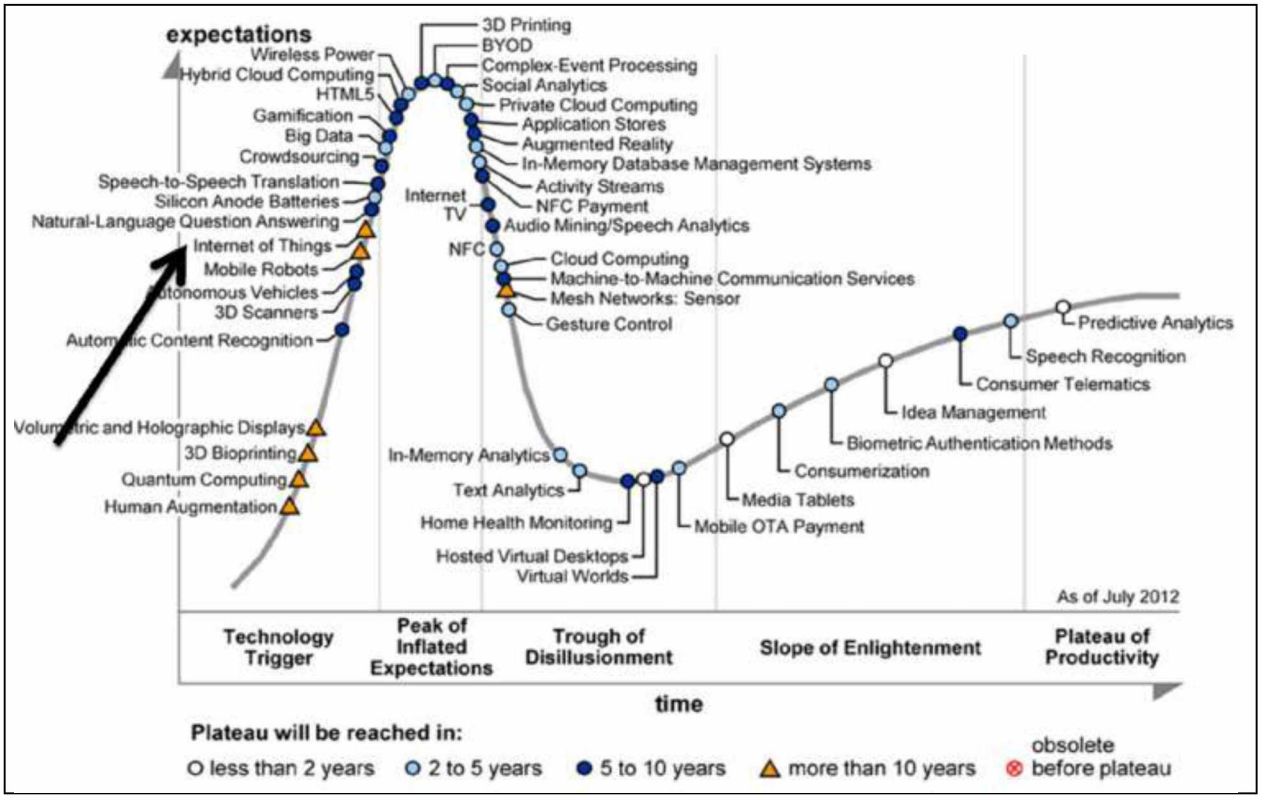
* Exigência legal Fonte: Schermer e Falot (2014).

Legenda:

+ +	As principais seções da política de privacidade adaptam-se muito bem, sendo coerentes com os requisitos.[17]
+	As principais seções da política de privacidade satisfazem os requisitos, mas ainda existem melhorias possíveis de serem feitas.
+ / -	As principais seções da política de privacidade encontram-se em padrões mínimos ou em pequenos itens pouco explorados e explicativos, havendo ainda muito espaço para melhorias.
-	As principais seções da política de privacidade não atendem aos requisitos.
- -	As principais seções da política de privacidade não são totalmente compatíveis com os requisitos e/ou não estão em cumprimento mínimo.

[17] Conforme informações encontradas nos termos do artigo 33 da Lei de Proteção de Dados - Código Civil do país em questão (Holanda).

Figura 6 – *Hype Cycle* de Gartner para tecnologias emergentes



Fonte: Gartner (2012).

De acordo com Gartner (2012), a IoT, bem como a internet TV, são tecnologias promissoras em utilização e ascensão nos últimos cinco anos e nos próximos dez que ainda estão por vir, conforme mostra a Figura 6, acima.

2.5 Direitos de uso do fabricante X direitos de uso do usuário

A famosa frase "*O direito de um começa onde termina o do outro*" deveria pautar a relação entre o fabricante de Smart TV e o usuário-cliente, mas infelizmente não é isso o que acontece. Alguns fabricantes ao menos se dão ao trabalho de elaborar e publicar sua política de privacidade, deixando claro (é o que se espera) para o usuário aquilo que será utilizado/armazenado como informação durante a interação dele com sua Smart TV. Acreditamos que os fabricantes deveriam manter o mesmo grau de coerência quando o

usuário manifesta o desejo de, por exemplo, instalar algum aplicativo que foge de certa forma ao "arcabouço" operacional do sistema desenvolvido para a Smart TV. No entanto, quando o usuário tenta fazer tal tipo de instalação não consegue, pois fica atestada uma "incompatibilidade", uma vez que ele não tem o direito de modificar o código fonte do sistema operacional da Smart TV para usufruir de outros recursos.

Essas restrições impedem que os usuários das Smart TVs possam acessar outros recursos midiáticos (por exemplo, novas *gadgets*) que eles tenham legalmente adquirido de outras fontes, conectando sua TV para a execução de aplicativos de sua escolha.

Além de tudo, essas restrições limitam a funcionalidade dos sistemas operacionais e aplicações *Free/Libre and Open Source Software* (FLOSS)[18] produzidos pelos membros da comunidade *open source* e outros desenvolvedores que os fabricantes não têm direito de restringir. Tais limitações minam a liberdade que os desenvolvedores de software FLOSS pretendem transmitir aos seus usuários.

Restrições a firmwares de Smart TV também representam um risco de segurança para seus proprietários-usuários. Pesquisadores e especialistas de segurança demonstraram recentemente uma série de vulnerabilidades na Samsung Smart TV que poderia dar condições aos hackers para acessar ou danificar remotamente o dispositivo de um usuário. Veremos alguns exemplos no próximo capítulo. Em alguns casos, esses problemas poderiam ser corrigidos ou mitigados pelo usuário com a instalação de um firewall ou outras contramedidas.

Existe uma organização sem fins lucrativos nos Estados Unidos chamada *Electronic Frontier Foundation* (EFF, 2016b), cujo objetivo é proteger os direitos de liberdade de expressão no contexto da era digital no mundo. De três em três anos, os grupos interessados podem propor isenções temporárias, conforme a Seção 1201 (EFF, 2016a), em um processo de regulamentação de tempo e mão de obra intensiva executado pelo Escritório de Direitos Autorais[19]. O *Software Freedom Conservancy*[20], em conjunto com o escritório de advocacia TorEkeland PC, propôs uma isenção para permitir que os usuários instalem softwares alternativos em suas Smart TVs sem autorização do fabricante. Enfim, essa organização pode

---

[18] Os termos software de código livre e aberto, ou *Free and Open Source Software* (F/OSS, FOSS), em inglês, e software de código livre/libre/aberto, ou *Free/Libre/Open Source Software* (FLOSS), referem-se a um software que é duplamente livre e de código aberto. Ele é livremente licenciado para conceder aos usuários o direito de uso, cópia, estudo, mudança e melhoria em seu design através da disponibilidade de seu código fonte. - Free Software Foundation. O que é um software livre? (O SISTEMA..., 2015).

[19] No caso, a EFF propõe seis classes de isenções.

[20] *Software Freedom Conservancy* é uma organização sem fins lucrativos que ajuda a promover, melhorar, desenvolver e defender *Open Source Software* (FLOSS). Projetos gratuitos, que oferecem, sem fins lucrativos, infraestrutura para projetos de software livre (SOFTWARE FREEDOM CONSERVANCY, 2015).

ser uma referência interessante para consultar, trocar informações e buscar orientações sobre essa dinâmica da falta de privacidade no meio digital.

2.6 Leis e regulamentos

Independente do segmento de mercado no qual esteja inserido (indústria, serviços, telecomunicações, dentre outros), é importante conhecer (como pessoa física ou jurídica) os regulamentos ou novos complementos regulatórios. No final dos anos de 1990 e 2000, criaram-se as primeiras leis que regem a segurança da informação, a privacidade e a prestação de contas, em parte em razão do grande volume de informações pessoais e confidenciais armazenadas e transmitidas por intermédio dos canais vulneráveis dos diversos segmentos de mercado existentes no mundo.

A intenção da maioria dos regulamentos é proteger a confidencialidade, integridade e disponibilidade da informação, levando-se em consideração os impactos que certas ameaças e vulnerabilidades podem trazer aos usuários-clientes. As leis podem ser destinadas para os seguintes objetivos essenciais:

a) criar e implementar controles;
b) manter, proteger e avaliar questões de conformidade;
c) identificar e corrigir vulnerabilidades e desvios;
d) fornecer relatórios que podem comprovar a conformidade da organização/fabricante.

Contemplaremos de forma sucinta no quadro abaixo as leis e os regulamentos que têm impacto imediato sobre os profissionais de tecnologia e negócios em geral (Quadro 6) para que possamos entender o que cada um aborda. Não se deve considerar esta lista como a representação final de todas as leis e regulamentos que podem se aplicar a determinado negócio, principalmente no que se refere às questões inerentes à proteção da privacidade de dados pessoais do usuário-cliente (NOBLETT, 2006).

Quadro 6 - Leis e regulamentos que impactam os profissionais de tecnologia e negócios

LEI/REGULAMENTAÇÃO	DESCRIÇÃO
Diretiva da União Europeia de Proteção de Dados (EUDPD)	Padroniza a proteção da privacidade de dados para os cidadãos de toda a União Europeia (UE), fornecendo requisitos básicos que todos os Estados-Membros devem respeitar em regulamentos nacionais. A EUDPD tem uma forte influência sobre os regulamentos internacionais em virtude das limitações que

	impõe ao envio de informações pessoais dos cidadãos europeus para fora da União Europeia, para áreas que são consideradas como tendo menos padrões adequados de segurança de dados. As diretivas e as regulamentações promulgadas em conformidade com a EUDPD impactam empresas que fazem negócios na UE ou que lidam com os dados dos cidadãos da UE.
California Senate Bill 1386 (CA SB 1386)	Foi introduzida em julho de 2003 como uma primeira tentativa de um legislador estadual para resolver o problema de roubo de identidade. Em suma, o projeto de lei introduz requisitos de divulgação rígidos para empresas e agências governamentais que sofram violações de segurança que possam pôr em risco as informações pessoais dos residentes da Califórnia. Espera-se que muitas organizações nos Estados Unidos estejam sujeitas a esses requisitos. Além disso, muitos outros estados detêm ou planejam aprovar uma legislação similar.
Proteção de Informações Pessoais e Documentos Eletrônicos (PIPEDA)	Regulamentação federal canadense que regula a utilização e divulgação de informações pessoalmente identificáveis no curso de transações comerciais. O ato foi criado em resposta às diretivas de proteção de dados da União Europeia que limitam o comércio com nações cuja proteção de privacidade não cumpra as normas da UE. A PIPEDA incorpora e torna obrigatórias as disposições da Associação Canadense de Normas do Código de modelo de Privacidade desde 1995. Essa lei abrange todo o Canadá, exceto aquelas províncias que possuem legislação "substancialmente similar" (ou seja, British Columbia, Alberta e Quebec), além de todas as províncias de comércio.

Fonte: Noblett (2006).

No Brasil ainda precisamos evoluir muito nesse sentido, com a criação de políticas públicas sustentadas por normas e procedimentos que possuam orientações mínimas para o relacionamento com empresas que entram em nosso país e não seguem adequadamente as leis de proteção ao consumidor, e que, sobretudo, não protejam a privacidade de suas informações, como acontece em outros países (Quadro 6).

> As diretrizes estratégicas explicitadas e qualificadas, que constituem o segundo nível da política de CT&I aqui formulada, identificam vias prioritárias para atingir os objetivos propostos. Estas diretrizes têm como ponto de partida a base de Ciência, Tecnologia e Inovação construída nas últimas décadas no Brasil, sucintamente caracterizada na seção anterior.

> Orientam-se para constituir a institucionalidade necessária para enfrentar o desafio da inovação, elemento determinante das políticas públicas em todo o mundo, que deve ser criativamente enfrentado pela sociedade brasileira (BRASIL, 2015).

Contudo, o Ministério de Ciência e Tecnologia do governo brasileiro, conforme menciona em seu Livro Branco (BRASIL, 2002), revela a importância de conduzir bem os desafios que a inovação tecnológica traz consigo, deliberando medidas estratégicas na esfera de políticas públicas, caso do novo Marco Civil brasileiro, que retrata algumas questões.

2.7 O Marco Civil da Internet brasileira e a privacidade

Com a Lei 12.965, conhecida como Marco Civil da Internet, busca-se regular o uso da internet no país como forma de garantir os deveres e a obrigação dos usuários da rede de computadores, no caso, a internet. O principal ponto da lei é a garantia dos direitos humanos como forma de fundamento da liberdade de expressão na rede mundial de computadores, essencial ao exercício da cidadania. No que se refere à construção dos direitos humanos, haverá sempre uma luta intensa para que eles sejam estendidos a todos os cidadãos. Com a vigência da Lei 12.965, espera-se que o respeito aos direitos humanos, como a privacidade e a liberdade de expressão na internet, seja verdadeiramente garantido. No entanto, é importante destacar que as garantias dadas por essa lei devem também sofrer os limites constitucionais mediante a necessidade de garantir o direito constitucional fundamental da personalidade e consequentemente a individualidade do cidadão nesse direito de escolha e definições.

A liberdade de expressão é fator preponderante para que se possa concretizar o chamado princípio da dignidade humana, uma maneira de proteger a sociedade da opressão. Os artigos 2º e 3º do chamado Marco Civil da Internet são bastante claros quanto à proteção dos direitos dos cidadãos e usuários de internet e consequentemente no que se refere aos princípios constitucionais civis, como se pode observar abaixo:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei (BRASIL, 2014).

A privacidade é o direito à proteção das informações pessoais e da própria vida privada. Na definição de Celso Lafer, é "o direito do indivíduo de estar só e a possibilidade

que deve ter toda pessoa de excluir do conhecimento de terceiros aquilo que a ela só se refere, e que diz respeito ao seu modo de ser no âmbito da vida privada." (LAFER, 1998).

Para Bastos (2000), o direito à privacidade é "a faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano". É justamente em virtude de tal direito que os fabricantes de Smart TV deveriam demonstrar mais responsabilidade com as informações de seus usuários que são trafegadas até os seus servidores ou terceiros. Acreditamos que as orientações do Marco Civil brasileiro nesta esfera deveriam prevalecer.

Na nova era digital, esse direito é muito vulnerável diante do imenso mundo da internet. Tendo como foco essa fragilidade, a lei de regulação da utilização da internet procurou proteger esse valor tão essencial para os usuários de rede móvel de computador, tanto em modo off-line quanto em modo on-line. Acreditamos que ele deveria se estender também para equipamentos inteligentes como a Smart TV, o que não está claro na lei. No que se refere à proteção da privacidade, o Capítulo II da Lei 12.965 trata dos direitos e das garantias dos usuários da internet apresentando um cunho mais voltado para a relação com o provedor do acesso à internet e não propriamente com o terceiro/fabricante em si.

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial [...]
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei (BRASIL, 2014).

O ministro Gilmar Mendes, do Supremo Tribunal Federal (FERREIRA, 2014), afirma em sua obra: "O termo vida privada se estende para além do mero direito de viver como se quer, livre de publicidade, para incluir também o direito de estabelecer e desenvolver relações com outros seres humanos".

Quanto ao direito à privacidade, o artigo 10 é bastante taxativo, destacando os cuidados que se deve ter ao arquivar todos os registros de conexão, bem como os dados pessoais das comunicações privadas.

> Art. 10 A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas (BRASIL, 2014).

Vejamos, por exemplo, algumas passagens da Seção III – "Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros".

> **Art. 18.** O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por **terceiros.**
> **Art. 19.** Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por **terceiros** se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.
> **Art. 21.** O provedor de aplicações de internet que disponibilize conteúdo gerado por **terceiros** será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo (BRASIL, 2014).

Percebe-se claramente que ainda deve haver um esclarecimento e amadurecimento maior nas tratativas referentes a esse terceiro, ou mais especificamente ao fabricante de equipamentos tecnológicos que utilizam, absorvem, captam, extraem, trafegam informações do usuário-cliente, mesmo que este tenha dado seu "consentimento" aprovando/aceitando a política de privacidade da empresa.

3 DETECTANDO AS VULNERABILIDADES NAS SMART TVS

Vamos partir aqui de algumas premissas deste mundo tão globalizado e transformador: "A informação é a alma do negócio". "Quem não se comunica está por fora". "A segurança da informação é vital". "A televisão é um meio de comunicação de massa". "Integrar e interagir é a melhor rede social". "Quem tem mais conhecimento tem mais poder'.

É fato que a Smart TV é popular no mundo inteiro (GARTNER, 2012). Em 2012, mais de 80 milhões de televisores inteligentes foram vendidos e a tendência é de que todas as classes sociais tenham pelo menos um em sua casa, tornando-se a Smart TV cada vez mais popular. Entretanto, existe uma certa dissonância entre essa inevitável popularidade e o nível de preocupação, conhecimento e atitude do usuário diante dos problemas de privacidade que uma TV inteligente pode trazer. Uma ausência de pesquisas de segurança neste contexto, a não percepção de que a Smart TV é como se fosse uma versão caseira do smartphone (tão utilizado hoje no mundo), sua utilização em diferentes campos do mercado (educacional, do entretenimento e de negócios em geral), todas as aplicações potenciais viabilizadas para serem utilizadas neste meio no mercado de eletrônicos de consumo e soluções diversas de tecnologia fazem com que ela esteja cada vez mais em evidência no mundo da Segurança das Informações.

Esta é uma realidade que se vive neste mundo globalizado e transformador, um mundo real e não virtual, em que os meios de comunicação mais poderosos, atrativos e com os quais estamos enormemente envolvidos em nossas rotinas de vida – a internet e a televisão – unificaram-se numa simbiose camaleônica dando origem à Smart TV.

Quando se fala em internet, há uma associação imediata com o universo computacional. E aquela distância que existia antigamente entre TV e Internet, que pareciam ser meios tão distintos e nada compatíveis numa interface de comunicação, diluiu-se numa modernidade "líquida", mas não superficial, de forma que a chance futura de os chamados *Personal Computers* (PC) ou *Desktops* serem extintos de vez, dando lugar à tecnologia cada vez mais inteligente dos novos aparelhos televisivos, agregados ao alto poder da *Cloud Computing* (computação em nuvem), é passível de acontecer sem nos darmos conta de tal "fenômeno".

Entretanto, neste contexto, há os perigos iminentes de novas (e até conhecidas) vulnerabilidades e ameaças internas e externas, mas agora tendo como foco não mais o PC em si, mas a Smart TV. Perigos esses que precisam ser combatidos e aos quais o usuário-cliente deve estar atento, já que o "inimigo" possui apenas um outro local de instalação e uso. Afinal,

por ser um tipo de equipamento de certa forma sofisticado e tecnologicamente evoluído, as Smart TVs estão espalhadas por diferentes tipos de lugares de grande relevância social, como aeroportos, hotéis, centros de convenção, centros culturais, de ensino e até mesmo religiosos, além, é claro, de nas próprias empresas.

Sendo assim, no presente trabalho, um dos nossos objetivos é entender a arquitetura desse poderoso meio de comunicação que é a Smart TV, os riscos existentes diante de algumas vulnerabilidades dos fabricantes que a produzem e lançam ao mercado, bem como as relações da convergência dos aplicativos e sinais de comunicação vigentes para esse tipo de tecnologia.

3.1 Sobre o *middleware* da TV digital

Antes de abordarmos diretamente as questões de segurança, é importante compreender um pouco a arquitetura e a composição da estrutura que permeia os aplicativos, o sistema operacional e consequentemente os serviços que transitam na Smart TV. O *middleware* é um termo abrangente, comumente utilizado para referenciar o software que atua como um mediador entre dois programas existentes e independentes. Seu objetivo é tornar as aplicações independentes do sistema de transmissão, possibilitando que inúmeros códigos de aplicações trabalhem com diferentes equipamentos de recepção, facilitando uma maior liberdade relacionada ao conteúdo transmitido. Por meio da criação de uma máquina virtual no receptor, os códigos das aplicações são compilados no formato adequado para cada sistema operacional. Resumidamente, podemos dizer que o *middleware* possibilita o funcionamento de um código para diferentes tipos de plataformas de recepção ou vice-versa, o que faz com que a plataforma JAVA, que nasceu sob essa perspectiva, se encaixe perfeitamente nele (PORTAL EDUCAÇÃO, 2015).

Pode-se dizer que o *middleware* se faz necessário para resolver o novo paradigma que foi introduzido com a TV digital: a combinação da TV tradicional (broadcast, ou transmissão de dados) com a interatividade, textos e gráficos. É justamente essa interatividade que trará várias características e funcionalidades encontradas no ambiente da Internet: representação gráfica, identificação do usuário, navegação diferenciada nos conteúdos e interações sistemáticas com ele; ou seja, tudo isso e mais um pouco daquilo que se encontra numa Smart TV. Entretanto, não se pode esquecer de que, independentemente do tipo de *middleware* que se vai definir nesse processo de interação entre software e hardware, é fundamental preocupar-se também com a transmissão daquilo que será trafegado. Por isso o protocolo TLS

(*Transport Layer Security*[21]) (DIERKS; ALLEN, 1999) é encontrado inclusive na TV Digital Interativa de modo a oferecer uma comunicação segura, para assim tentar mitigar os riscos da perda de um dos princípios da segurança da informação, que é a integridade e autenticidade (EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE, 2003).

> Os desenvolvedores de aplicações deixaram de se preocupar com os protocolos existentes nas camadas inferiores do sistema de transmissão e focalizaram uma interface padrão para desenvolvimento de seu trabalho. JAVA é um formato aceito na maioria dos middlewares em funcionamento (PORTAL EDUCAÇÃO, 2015, p.79).

O que se sabe atualmente é que até agora não há, de fato, um padrão de *middleware* universal. Existem três grupos que buscam formalizar um padrão aberto: a Europa, com o sistema DVB, que tenta padronizar o MHP; os Estados Unidos, com o ATSC, que tenta a evolução do DASE; e o Japão, com o ISDB, que tenta o ARIB.

Quadro 7 – Comparação dos padrões de *middleware*

CARACTERÍSTICA	MHP	DASE	ARIB
Segurança	Sim	Sim	Não disponível
Decodificação de conteúdo comum (PNG, JPEG, ZIP etc.)	Sim	Sim	Sim
Tipos de aplicativos	HTML e JavaTV	XHTML,CSS,ECMA Script, JavaTV	Não disponível
Distinção entre aplicações declarativas e procedurais	Sim	Sim	Não disponível
Interação com o usuário	Sim	SIM (teclado, mouse)	Sim
Capacidade de áudio	MPEG BC	Non-streaming: (audio/basic) Streaming: (Dolby AC-3)	Sim
Capacidade de vídeo	MPEG 2	Non-streaming: (Multiple Network Graphics) Streaming: (MPEG 2)	MPEG 2
Capacidade gráfica	LDTV: 320 X 240 SDTV: 640 X 480 EDTV: 720 X 480 HDTV: 1920 X 1080	1920 X 1080 1280 X 720 960 X 540 640 X 480	Alta definição: 1920 X 1080; 1280 X 720 e 960 X 540. Definição normal: 620 X 480.

[21] *Transport Layer Security* (TLS) é um protocolo que fornece privacidade e integridade de dados entre dois aplicativos que se comunicam. É a segurança mais amplamente implantada, sendo o protocolo mais usado hoje em navegadores da Web e outras aplicações que requerem dados a serem trocados de forma segura por meio de uma rede, tais como transferências de arquivos, VPN ligações, mensagens instantâneas de voz sobre IP.

Display	Não disponível	Multiplano: background, vídeo, gráfico e ponteiro/cursor (8 bits pseudo color; RGBA 4444; RGBA 5551; RGBA 6666; RGBA 8880 e RGBA 8888)	Multiplano: vídeo, figura, controle, gráfico, texto e legendas: (Y, Cr,Cb/4:2:2/8bits;Y, Cr, Cb/4:4:4/8bits/ composição do canal α em 256valores;1920 X 1080 X 1 - 1 bit de controle; 8 bits para endereçamento de mapa de cores) Correção de erros sem perda
Metadados	Sim	Sim	Sim
Receptor (STB)	Receptores comuns de baixo custo	Receptores comuns	Receptores comuns de baixo custo
Extensões/Expansões	Sim	Não disponível	Sim
Serviços	HDTV, SDTV, outros serviços de telecomunicações e de dados	HDTV, SDTV, outros serviços de telecomunicações e de dados	HDTV, SDTV, outros serviços de telecomunicações e de dados
Interatividade	Sim	Sim	SIM, via digital broadcasting, SDTV (terrestre), satélite, redes de pacotes e redes de telecomunicações
Controlabilidade	Funções de controle do usuário; canais de emergência	Controle do usuário	Funções de controle do usuário; canais de emergência
Vantagens	Baixo preço do Set Up Box; maior aceitabilidade mundial	Possibilidade de contrapartidas comerciais nos EUA	Melhor para aplicações móveis; proximidade funcional com DVB (Digital Vídeo Broadcasting)

Fonte: Paes e Antoniazzi (2005).

É extremamente importante compreender que, sendo o *middleware* um s*oftware* que intermedeia e funciona como uma espécie de emulador entre os programas, algumas vulnerabilidades podem ser exploradas por seu intermédio, como atualizações de firmware, da passagem de diretórios (pastas de armazenamento que a Smart TV contém internamente), execução de códigos (elaboração de *script shell*), bem como JTAG (*Joint Test Access Group*) ou leitura física NAND/SD (*Flash Memory*).

Quando se fala da arquitetura da TV digital, mais especificamente da Smart TV, é impossível não discutirmos as questões relativas ao *middleware*, como citamos anteriormente, relacionadas aos cuidados de segurança quando se usa JAVA, e o que a *Multimedia Home Platform* (MHP), bem como a DASE - *DTV Application Software Enviornment* e o *Association of Radio Industries and Business* (ARIB) podem fornecer como padrão de

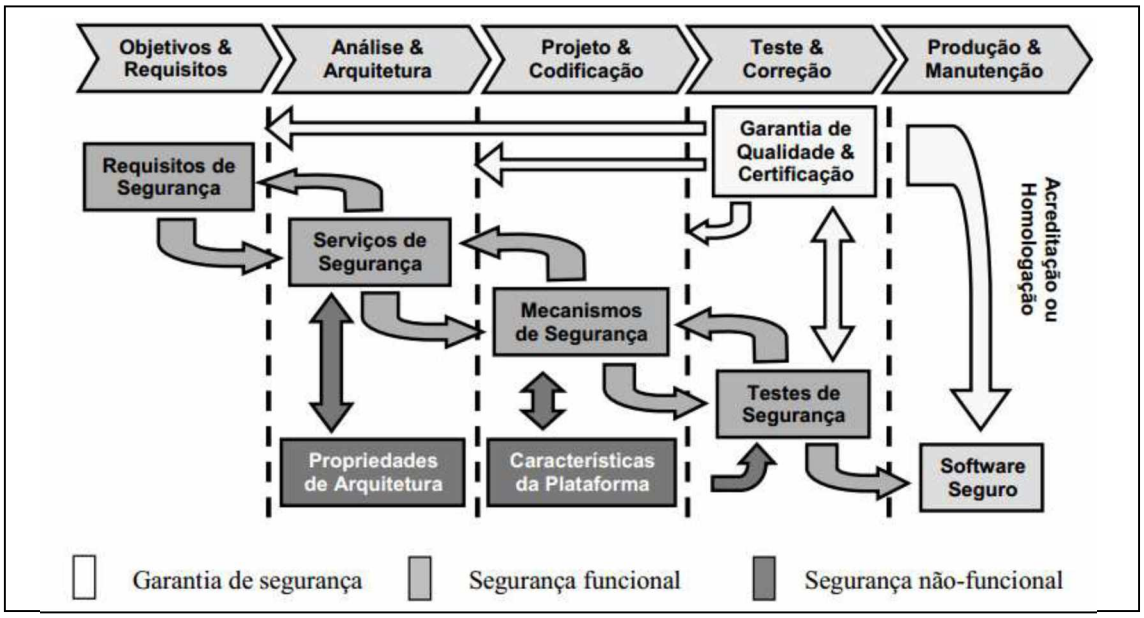
segurança. Não vamos aqui nos preocupar profundamente com esses conceitos, pois não é nosso intuito, além de ser algo tecnicamente muito específico, que seria mais apropriadamente explorado em outro trabalho. Todavia, é importante saber que existem tais padrões de *middleware* com características, funções e objetivos distintos e alguns, de fato, com foco mais voltado para a segurança. Eles podem ajudar novos pesquisadores a desenvolver frameworks que proporcionem a geração de aplicativos seguros para a transmissão no canal de interatividade da TV digital, contribuindo assim para uma melhor compreensão da definição dos mecanismos necessários para se obter segurança.

Não discutiremos o contexto específico de determinado *middleware* utilizado no desenvolvimento de uma Smart TV, como o Ginga, aqui no Brasil, bem como outro padrão de arquitetura qualquer, nem o mérito de qual é melhor ou pior. Não se pretende, neste trabalho, explorar ou esgotar tal assunto, pois não é esse nosso propósito. Consideraremos genericamente o *middleware* como um todo, como uma parte integrante da arquitetura que formará, junto com as aplicações, o sistema operacional, os dispositivos, o hardware e as melhores práticas para mitigar riscos de segurança, prevenindo-se as possíveis ameaças por meio de uma formação mais robusta, consistente e confiável contra as vulnerabilidades que poderiam ser facilmente exploradas.

Para tanto, não basta lá na ponta do processo (a utilização final do cliente) que o usuário possua a consciência de que é preciso haver uma configuração segura e preventiva daquilo que ele encontrará como recurso nativo, um padrão de fábrica já instalado na Smart TV, se toda a arquitetura construída e que chega ao usuário-telespectador vier com falhas ou possibilidades engessadas de futuras atualizações e correções lógicas.

Por isso, mais do que nunca, é essencial estabelecer um *framework* de desenvolvimento seguro de software, pois é justamente essa parte lógica que fornece todo o mecanismo operacional e funcional da interface de configuração e interação TV-usuário, fazendo uma grande diferença no quesito de proteção e, claro, de maior privacidade.

Figura 7 – Processo de desenvolvimento seguro de software



Fonte: Braga e Restani (2010).

Sem dúvida, a segurança é um aspecto da qualidade dos sistemas que interage com o usuário. E, nesse sentido, a inserção da segurança de forma preventiva no desenvolvimento dos sistemas estabelece uma maior confiança num produto final de qualidade que será oferecido e chegará ao usuário, que muitas vezes ignora as possíveis vulnerabilidades que pode ter ao possuir em sua rede uma Smart TV conectada à internet. É complicado afirmar que não haverá falhas, contudo uma maior confiança e qualidade no processo de desenvolvimento do software proporcionaria uma maior garantia de qualidade e controle de estabilidade diante das camadas de software e hardware que formam os multisserviços de uma Smart TV, chamada assim de produto final. A Figura 35 apresenta um processo de desenvolvimento seguro de sistemas, retratando um fluxo de segmentação nos aspectos de segurança funcional (mais flexível, por não depender do fabricante) e segurança não funcional (por depender mais daquilo que vem do fabricante), buscando assim maior e melhor garantia de qualidade com um processo de arquitetura mais segura.

É interessante destacar que os padrões de *midlware*, conforme apresentados no Quadro 7, possuem claramente características diferentes. Mas, independentemente disso, prover segurança é estabelecer padrões uniformes para qualquer tipo de arquitetura, uma vez que as vulnerabilidades são exploradas em virtude de dois fatores básicos: a falta de recursos padrões de proteção (aqui entram os protocolos de segurança) e a existência de recursos defasados/desatualizados.

3.2 A sinergia entre segurança, convergência e os sinais de comunicação

O surgimento de tanta tecnologia similar com intuitos finais muito semelhantes ou até mesmo com propósitos iguais de resultados entregues ao usuário faz com que o poder da convergência extrapole as barreiras do ostracismo digital. Com a chegada dos inúmeros tipos de adaptadores e dispositivos para streaming de mídia digital – os set-top-box, HTPC'[22], e tantos outros na Internet das Coisas – e o surgimento de tanta pesquisa, inovações tecnológicas e a febre de startups[23] entramos na Matriz que Henry Jenkins retrata muito bem em seu livro *Cultura da convergência*, o que nos fez perceber o quão difícil é selecionar e diferenciar o que pode ser realmente bom ou não. Dificuldade essa que se revela na escolha de produtos, serviços e soluções, neste momento mais do que nunca, visto que as Smart TVs vieram para ficar e trazem consigo esse poder da convergência, centralizando uma série de recursos digitais e tecnológicos oferecidos pelos diversos tipos de equipamentos da esfera transmidiática.

É neste contexto que surgem os perigos com a segurança das informações em razão do descompasso entre a evolução do poder de convergência dos novos recursos para as Smart TVs, e as novas vulnerabilidades que surgem em função da interação, mobilidade, integração e acessibilidade que se apresentam para o usuário.

Existem dois tipos de protocolos de comunicação que emitem sinais de frequência adequados para estabelecer os comandos dados por alguns recursos presentes na Smart TV. Esses dois protocolos são chamados **ZigBee** e **Z-Wave** (Quadro 8), tecnologias sem fio e de curto alcance, utilizadas para monitoramento e controle remoto. No entanto, as respectivas especificações e aplicativos são diferentes. Ambas as tecnologias são ideais para redes de área-home (Hans), que estão se tornando mais difundidas em nosso meio.

O Z-Wave é focado principalmente em funções de monitoramento e controle em casa e em pequenas instalações comerciais. É amplamente utilizado para o controle de iluminação, segurança e temperatura. Outros usos incluem detectores de fumaça, fechaduras, sensores de segurança, aparelhos e controles remotos. Ele é também normalmente utilizado em alguns medidores elétricos inteligentes para fornecer dados de consumo para monitores e controles de HVAC (aquecimento e ventilação de ar condicionado) em casa.

---

[22] Acrônimo de *Home Theater Personal Computer* (HTPC). Um PC *home theater* ou media center computador é uma convergência do dispositivo que combina algumas ou todas as capacidades de um computador pessoal com uma aplicação de software que suporta vídeo, foto, reprodução de áudio e, algumas vezes, gravação de vídeo.

[23] *Startup* significa o ato de começar algo, normalmente relacionado com companhias e empresas que estão no início de suas atividades e que buscam explorar inovações no mercado.

Já quanto ao ZigBee, um de seus grandes benefícios é a flexibilidade. Ele foi projetado de modo que o software aplicativo possa reconhecer diversos perfis, tornando mais rápido e fácil para os fabricantes criar produtos sem fio para aplicações muito específicas. Os perfis disponíveis incluem automação residencial, energia inteligente, telecomunicações, cuidados de saúde, controle remoto (conforme padrão RF4CE[24] para frequência de rádio e eletrônicos de consumo, como Smart TV), automação predial etc. A grande questão é a coexistência com Wi-Fi e Bluetooth, que usam a mesma banda. A maioria dos transceptores possuem algum mecanismo de redirecionamento para minimizar a interferência (ELETRONICDESIGN, 2015).

Quadro 8 - Especificações e capacidades de sinal das tecnologias ZigBee e Z-Wave

Tecnologia	Frequência	Modulação	Taxa de dados	Alcance	Aplicações
ZigBee	2.4 até 2.483 Ghz	OQPSK	250 Kbits/s	10m	Domótica, redes inteligentes, controle remoto
Z-Wave	908.42 Mhz	GFSK	9.6 / 40 Kbits/s	30m	Domótica, segurança

Fonte: Eletronicdesign (2015).

É preciso, entretanto, estar atento à flexibilização dos protocolos, que podem ser perigosos no sentido de possíveis interferências no sinal de comunicação da Smart TV, por esta utilizar justamente esses dois tipos de sinais, Wi-Fi e Bluetooth, que outros meios também utilizam. Levando-se em consideração toda essa nova dinâmica da IoT e a convergência digital, com os inúmeros processos de automação residencial existentes e a vertente da domótica[25], é comum que vários outros recursos on-line (geladeira, micro-ondas,

[24] A RF4 Control, plataforma da Atmel compatível com ZigBee RF4CE, é cheia de recursos. O padrão ZigBee RF4CE aprimora o padrão IEEE 802.15.4, fornecendo perfis de aplicação padrão e camadas de rede simples, que podem ser usadas para criar uma solução operável por vários fornecedores para bens de consumo eletrônicos (EC). O pacote de software RF4Control oferece suporte a toda RF da Atmel Soluções em chip único e Transceptores de Rádio, e estende a operação para 2,4GHz em conformidade com as normas ao suportar a mesma funcionalidade e recursos para a frequência de banda de 900MHz (ATMEL, 2016).

[25] Tecnologia responsável pela gestão de todos os recursos habitacionais. Esse termo nasceu da fusão da palavra "domus", que significa casa, com a palavra "robótica", que está ligada ao ato de automatizar, isto é, de realizar ações de forma automática

smartphones, wearables[26], dentre outros eletros da linha branca) possam causar alguma interferência.

3.3 Aplicativos e o sistema operacional

Para a construção de aplicativos, de sistema operacional para a Smart TV, plataformas de segurança e padrões aderentes para esse fim, alguns *frameworks* de desenvolvimento devem ser considerados para estudo e pesquisa e na codificação com segurança (Quadro 9).

Quadro 9 – Frameworks de desenvolvimento considerados na codificação com segurança

PLATAFORMA	CARACTERÍSTICA	ONDE ENCONTRAR
Samsung SDK	Suporta Java, HTML, Adobe AIR	samsungdforum.com
LG SDK	Suporta HTML, Adobe AIR, Unity	developer.lgappstv.com
Google TVDK	Suporta Java, HTML, Adobe AIR, Unity.	developers.google.com/tv/android
SmartTV Alliance SDK (LG, a Sharp, Philips)	Suporta HTML	smarttv-alliance.org
NetTVDK (Sharp, Philips)	Suporta HTML	yourappontv.com
Roku SDK	Suporta C++, Unity	roku.com/developer
PlayJam SDK	Suporta Adobe AIR, executa dentro de LG e Samsung (e apoia o suporte a HTML)	playjam.com
TV App Engine	Suporta HTML e converte aplicativos para os padrões nativos	tvappagency.com
Marmalade	Suporta C/C++ e integrações com PlayJamAPIs	madewithmarmalade.com
Yahoo Connected TV	Suporta HTML	connectedtv.yahoo.com/developer
Opera TV	Suporta HTML	dev.opera.com/tv

Fonte: Stack Overflow (2016).

[26] Conhecido como "tecnologia vestível", são eletrônicos que podem ser usados no corpo, como acessório ou como parte de material usado em roupas. Uma das principais características da tecnologia *wearable* é a sua capacidade de se conectar à Internet, permitindo que os dados sejam trocados entre a rede e o dispositivo.

3.4 Vírus

Entramos aqui num questionamento que instiga não somente os fabricantes de Smart TV, como também os especialistas em segurança da informação. Afirmar categoricamente que não existe nenhum tipo de *malware* para Smart TV é no mínimo arriscado. Considerando que a categoria *malware* vai além dos vírus, sendo constituída de arquivos maliciosos que poderiam adentrar ou invadir a Smart TV, poderíamos talvez afirmar com maior convicção que não há um tipo de contaminação padrão e universal para todo tipo e fabricante de Smart TV, assim como acontece naturalmente com os Sistemas Operacionais para computadores. Pelo menos por enquanto. E sãos alguns os fatores que podem contribuir para essa situação: a fragmentação dos sistemas operacionais; a lenta adesão da população às televisões inteligentes, pelo menos em países ainda não tão desenvolvidos e economicamente estáveis, bem como a pluralidade de softwares existentes no mercado, em que cada fabricante possui um sistema operacional próprio para controlar a TV. Sendo assim, a disseminação de um vírus atingiria apenas um número menor de aparelhos, facilitando o controle e diminuindo os resultados para os criminosos.

> Para os criminosos virtuais a base de usuários de Smart-TV ainda é pequena e não compensa", aponta Fabio Assolini, analista sênior de malware da Kaspersky Lab. De acordo com o especialista, à medida que cada vez mais pessoas optem pelas TV inteligentes, aparecerão vírus que afetem os aparelhos. (RIBEIRO, 2014, p. 92).

Desta forma, como não se tem ao certo uma detecção oficializada de contágio de nenhum tipo de vírus ou *malware* qualquer, as empresas de segurança e antivírus, bem como as próprias fabricantes de Smart TV, não investiram ainda em recursos pesados para a criação de ferramentas que combatam exclusivamente ameaças direcionadas a ela, por não saberem exatamente do que se proteger. Mas deve ficar bem claro que não é porque ainda não se tem um foco de ataque externo de vírus ou de demais *malwares* direcionados para a Smart TV que sua segurança está garantida. O grande problema a ser explorado não são por enquanto tais ameaças, mas sim as vulnerabilidades internas que já vêm de fábrica nos aparelhos colocados no mercado.

> - Uma das pesquisas mais contundentes sobre as brechas das TV inteligentes foi realizada em 2012. Pesquisadores da ReVulN, empresa de teste de software com sede em Malta, na Europa, conseguiram controlar remotamente todas as funções de uma Smart TV Samsung, como trocar

> de canal, ligar e desligar e até mesmo acessar os arquivos de um pen-drive.
> - Outro problema aconteceu com uma Smart TV LG, também em 2012. Um usuário estava desconfiado das publicidades que apareciam no sistema e resolveu analisar a fundo o código do aparelho. Ele descobriu que a própria LG estava vasculhando os nomes dos arquivos do pen-drive.
> - Um estudo realizado pelo Network Security Lab da Universidade de Columbia, de Nova York, EUA, revelou o quanto as TV conectadas estão expostas ao ataque de hackers. Gastando apenas US$ 450 – pouco mais de R$ 1 mil – é possível construir um drone com um captador de sinal para roubar informações das TV inteligentes. Chamado de Red Button Attack, ao sobrevoar uma área de 1,4 km o equipamento consegue captar dados – como o login do Facebook e informações bancárias, por exemplo – de 20 mil TVs, explorando uma vulnerabilidade no HbbTV, tecnologia de transmissão de sinal de TV bastante comum na Europa. (RIBEIRO, 2014).

Contudo, algumas precauções podem mitigar certos riscos e proteger os usuários, se forem tomadas algumas contramedidas inerentes a essas ameaças e vulnerabilidades, como, por exemplo:

a) **Atualizar o firmware**: mantenha sua Smart-TV sempre atualizada. Alguns aparelhos possuem a opção de atualização automática. Ative essa função.

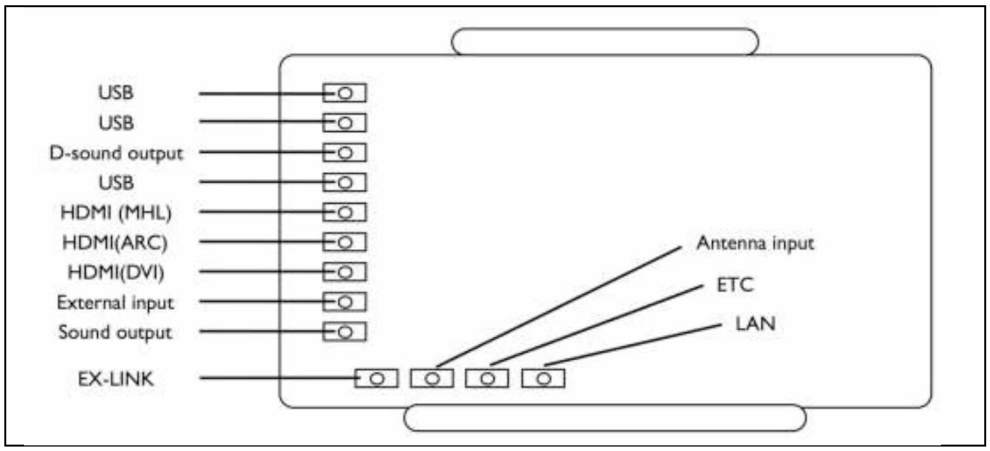
b) **Blindar o roteador**: procure manter a criptografia mais atual. Roteadores mais antigos possuem encriptação WEP, antiga e mais suscetível à invasão. Dê preferência a dispositivos com o protocolo de segurança WPA2, mais atual e seguro.

c) **Evitar compras**: não coloque informações de cartões de crédito, dados bancários ou faça compras pela Smart TV. Elas não possuem sistema de verificação SSL, ou seja, não é possível verificar se o *site* é confiável.

d) **Suspeitar de determinados links:** assim como em outras plataformas, evite clicar em links desconhecidos, mantendo o mesmo padrão quando navega em seu computador.

e) **Ter cuidado com dados externos**: use com cautela pen drives e HDs externos. Antes de conectá-los à TV, passe um antimalware. Também proteja dados sensíveis dos dispositivos, utilizando algum software de criptografia. Ou seja, além dos perigos iminentes que vêm da internet, existe a possibilidade de infecções por intermédio dos componentes da própria Smart TV, como demonstra a Figura 8.

Figura 8 – Processo de desenvolvimento seguro de software



Fonte: KoreaUniversity (2013).

3.5 Os vetores de ataque

Antes de tudo, é essencial entender os grandes obstáculos que dificultam a busca de informações de pesquisa para a Smart TV. Entre eles, temos:

a) a falta de documentação e pesquisa a respeito – grande superficialidade técnica, procedimental e operacional;
b) a TV é *blackbox*, de maneira que a janela de navegação é a própria tela que está integrada ao modo lógico e físico (*hardware* e *software*);
c) o fabricante da Smart TV engessa o código fonte dificultando o acesso, ficando centralizado somente nele o que se codifica e determina;
d) é difícil encontrar lugares interessantes para trocar ideias e experiências, bem como especialistas em Smart TVs;
e) as experiências práticas são elementares e nada instrutivas, e não se tem garantia nem com o reset de fábrica, pois ele pode não funcionar;
f) dificuldade de interação, pois o usuário é obrigado a enviar a Smart TV somente para o centro de assistência autorizada para ter diagnósticos e laudos técnicos. O próprio fabricante não se manifesta.

Podemos assim dizer que a Smart TV tem quase os mesmos vetores de ataque que um celular-smartphone, considerando os riscos de acesso indevido. Por exemplo, um hacker poderia

a) enviar aplicativos maliciosos para o seu provedor de aplicativos (apps) da Smart TV;
b) acessar fora da sua rede;

c) acessar dentro da sua rede ou mesmo interceptar alguma informação;

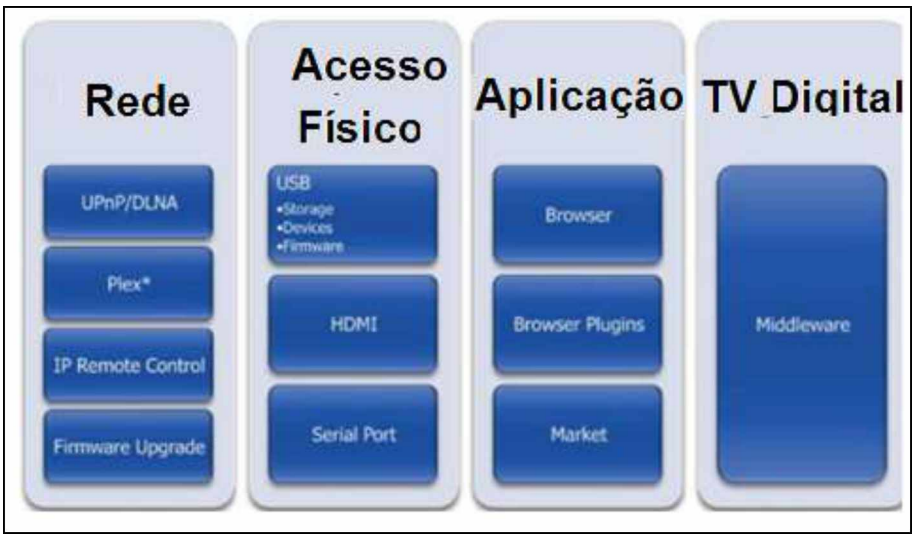
d) acessar sua TV (ataques físicos: USB etc.);

e) ver a sua TV (controle remoto);

f) estar próximo à sua casa/empresa (sinais de transmissão).

De forma geral, os principais silos que compõem os vetores de ataque estão presentes nas quatro dimensões a seguir: rede, acesso físico, aplicações e TV digital. Tal situação pode ser observada na Figura 9.

Figura 9 – Vetores de ataque



*Plex[27] Fonte: Espinhara e Albuquerque (2016).

Um outro problema, este presente especificamente nas Smart TVs, é o recurso UART[28], que por padrão fica habilitado por intermédio do controle remoto (e aqui não somente o que vem originalmente de fábrica, como também os chamados controles remotos universais), podendo enviar sinais à TV que poderiam causar certos transtornos, havendo a possibilidade de entrar em alguns modos de serviço do aparelho. Por exemplo:

a) desligue sua Smart-TV + Botão Mute + 1 + 8 + 2 + Power On;

b) ao ligar em seguida a televisão surgirão na tela algumas informações de fábrica, contendo inclusive a opção "*Advanced Mod*" (Modo avançado);

c) com isso, algumas configurações de fábrica podem ser alteradas.

---

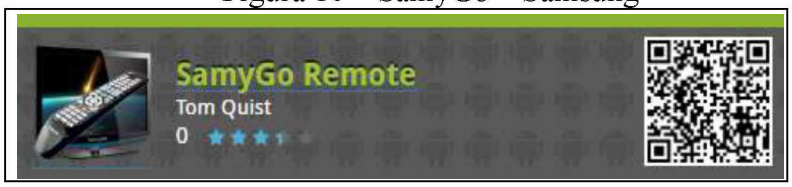
[27] O Plex é um *Media Center* multiplataformas que permite que os seus usuários realizem *streaming* de conteúdo de um dispositivo para outro que esteja na mesma rede *wireless*, sem custo para *laptops* e TV. Para quem usa celulares e *tablets*, é preciso pagar pelo aplicativo móvel para iOS ou Android.

[28] UART é o acrônimo de *Universal Asynchrounous Receiver Transmiter* ou Transmissor Receptor Universal Assíncrono. Sua finalidade é possibilitar a transmissão e a recepção de dados originalmente disponíveis na forma paralela.

Existe, porém, uma situação que pode ser enxergada por um ângulo diferente, que é a utilização "ingênua" dos Apps (aplicativos para *mobile*) para o controle remoto via celular-*smarthpone*, um recurso interessante e às vezes muito útil, quando se perde o controle remoto original ou quando ele estraga. Possuindo essa função ele pode ser utilizado com intuitos diferentes por pessoas mal-intencionadas para atrapalhar ou causar algum tipo de transtorno ao espectador ou público que esteja assistindo à Smart TV. A seguir, destacam-se alguns exemplos que podem ser baixados no *Google Play* para *Android*.

a) **SamyGo – Smart TV samsung**: o *Smart Remote* é um aplicativo gratuito e oficial da fabricante sul-coreana compatível praticamente com todas as televisões da Samsung. Para que o **SamyGo** funcione, basta que seu dispositivo Android esteja conectado na mesma rede da Smart TV, visto que a comunicação funciona via LAN.

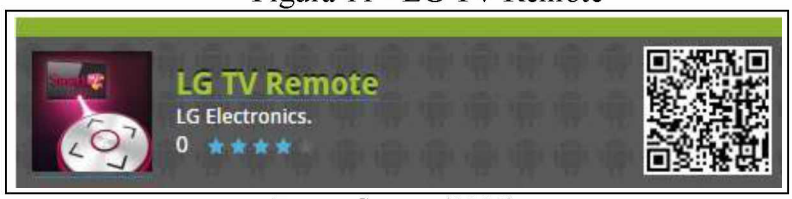
Figura 10 – SamyGo – Samsung



Fonte: Soares (2015).

b) **Smart TV LG**: o *LG TV Remote* é o aplicativo oficial da LG para controlar a Smart TV via dispositivo Android. Na *Play Store* existem "dois aplicativos oficiais", mas não é preciso se preocupar, pois a LG oferece uma versão para as Smart TVs lançadas até 2011 e outra para televisores lançados a partir de 2012.

Figura 11 - LG TV Remote



Fonte: Soares (2015).

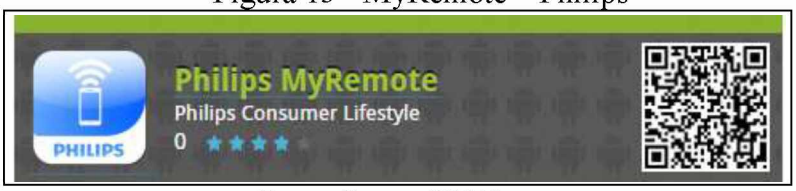
c) **Smart TV PANASONIC**: a Panasonic também figura na *Play Store* com dois aplicativos oficiais, o Panasonic TV Remote e o Panasonic TV Remote 2. A única diferença entre eles é que a primeira versão suporta TVs dos anos 2011/2012, e a segunda, além destas, também os modelos atuais. O usuário pode testar ambos casos tenha uma Smart TV fabricada em 2011 ou 2012.

Figura 12 - TV Remote – Panasonic

Fonte: Soares (2015).

d) **Smart TV PHILIPS**: o aplicativo ***Philips MyRemote*** não funciona apenas como controle remoto; ele transforma seu Android em uma central de entretenimento graças às funções de streaming entre smartphone/tablet e sua Smart TV, permitindo que o usuário reproduza vídeos e fotos instantaneamente.

Figura 13 - MyRemote – Philips



Fonte: Soares (2015).

e) **Smart TV SONY**: a usabilidade do ***TV Side View*** da Sony é um dos pontos fortes do aplicativo que, além de permitir o controle da TV por dispositivos móveis, também oferece guia de programação e possui compatibilidade estendida para outros aparelhos da Sony.

Figura 14 - TelecomandoTV – Sony

Fonte: Soares (2015)

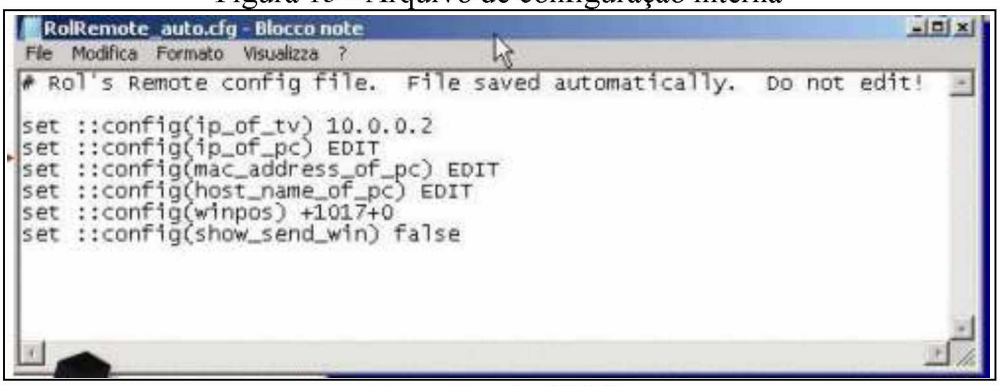
3.6 As vulnerabilidades

Com base em diversas pesquisas documentais e exploratórias com referências de estudo em laboratórios por entidades e pesquisadores especializados em segurança de Smart TVs, conseguiu-se levantar informações que relatam algumas experiências realizadas. Dentre

elas, iremos apresentar aqui algumas situações ocorridas com dois diferentes fabricantes de Smart TV: Samsung e Phillips. Isso não significa que apenas essas TVs possuam vulnerabilidades, eximindo outras marcas/modelos.

- **SAMSUNG**
  - **Aparelho testado:** Samsung Smart TV D6000 / 2012
  - **Serviço/Protocolo afetado:** consegue-se enviar solicitação HTTP por intermédio das portas de conexão (52253 e 52396).
  - **Vulnerabilidade:** exploração do acesso aos diretórios para baixar os arquivos disponíveis dentro da Smart TV.

Figura 15 - Arquivo de configuração interna



Fonte: Revuln (2016).

Com base no acesso dos arquivos de diretório interno da Smart TV (por exemplo, o que está representado na Figura 15 (RolRemote_auto.cfg), que são arquivos importantes de configuração) é possível falsificar o IP, o endereço MAC e o nome do host para permitir que um invasor na rede possa representar o controlador de TV na lista de permissões.

- **PHILLIPS**
  - **Aparelho testado:** todos os modelos da Phillips / 2013
  - **Serviço/Protocolo afetado:** acesso UDP (via rede LAN) aos serviços de TV.
  - **Vulnerabilidade:** codificação de senha fixa/padrão "miracast" e exploração do acesso aos diretórios para baixar os arquivos disponíveis dentro da Smart TV pelo *Joint Space* (aplicativo remoto da própria fabricante).

Utilizando o próprio controle remoto e o aplicativo padrão *Joint Space*, consegue-se acessar os diretórios que contêm arquivos de configurações importantes da Smart TV sem a necessidade de nenhum tipo de PIN para autenticação/identificação do suposto solicitante, e com acesso à senha pré-fixada.

Uma forma de avaliar as vulnerabilidades das redes, softwares e dispositivos em que a Smart TV está inserida é por meio da simulação de ataque conhecida como *fuzzing*, que nada mais faz do que emular a pirataria por parte de sistemas e aplicações, seja em casa ou nas empresas, com entradas defeituosas e inesperadas que propositalmente entram implacavelmente, expondo assim as falhas. Um fornecedor da solução que oferece uma plataforma de *fuzzing* é a *Codenomicon*, que se associou à Telcordia em 2011 para ajudar a comercializar o seu serviço de defesa para testes de vulnerabilidades desconhecidas. Como se pode observar na Figura 16, são inúmeras as formas de ataque que podem ser exploradas, inclusive as já supracitadas.

Figura 16 - Formas de exploração das vulnerabilidades

Fonte: Pipeline Publishing (2016).

A *Codenomicon* efetuou testes de *fuzzing* em seis Smart TVs com seis protocolos diferentes. Os resultados, tal como ilustrados no Quadro 10, demostram que todos os fabricantes (*vendors*) possuem dispositivos que podem ser comprometidos por sinalizações/acessos inesperados.

Quadro 10 – Análise de segurança por fabricante

Protocolo	Fabricante 1	Fabricante 2	Fabricante 3	Fabricante 4	Fabricante 5	Fabricante 6
IPv4	pass	fail	fail	pass	pass	fail
DVB	fail	fail	fail	Fail	fail	fail
UPnP	n/a	fail	pass	n/a	n/a	fail
Images	pass	fail	fail	n/a	n/a	fail
Audio	pass	pass	n/a	n/a	n/a	pass
Video	fail	fail	pass	Fail	fail	fail

Fonte: Pipeline Publishing (2016).

Legenda:

- pass = não vulnerável
- fail = vulnerável
- n / a = não disponível para testes

A técnica *fuzzing* também pode ser usada para expor vulnerabilidades em *Bluetooth*, bem como em Ethernet, VoIP, LTE, IMS, XML e em centenas de outros protocolos, de forma que a engenharia e o laboratório de soluções técnicas dos fornecedores podem utilizá-la para fazer testes preventivos antes de homologar seus aparelhos para entrar em produção.

É fundamental, portanto, que o cliente, usuário ou telespectador tenha conhecimento da existência de possíveis vulnerabilidades, assim como das possibilidades de ameaças e de todos os cuidados preventivos de conduta e configuração que podem ser realizados em sua Smart TV.

4 DADOS/PLANO DE APLICAÇÃO

O projeto em questão refere-se ao desenvolvimento de um aplicativo mobile para celulares e smartphones compatível com sistema Android, uma das plataformas mais utilizadas no mundo. A proposta é que se possa fazer o download desse aplicativo gratuitamente no Google Play em qualquer lugar que tenha conexão com a internet.

A necessidade primeira deste projeto foi entender qual a plataforma mais adequada para o desenvolvimento do aplicativo, com conversão mobile e aparatos compatíveis com testes, avaliações, simulações e homologação.

As atividades previstas antes da execução do projeto foram basicamente:

a) levantamento dos requisitos;
b) desenho da estrutura do aplicativo;
c) estudos sobre recursos técnicos compatíveis para gerar a APK;
d) definição da plataforma e linguagens;
e) elaboração do referencial teórico;
f) fomentação do conteúdo a ser inserido no aplicativo.

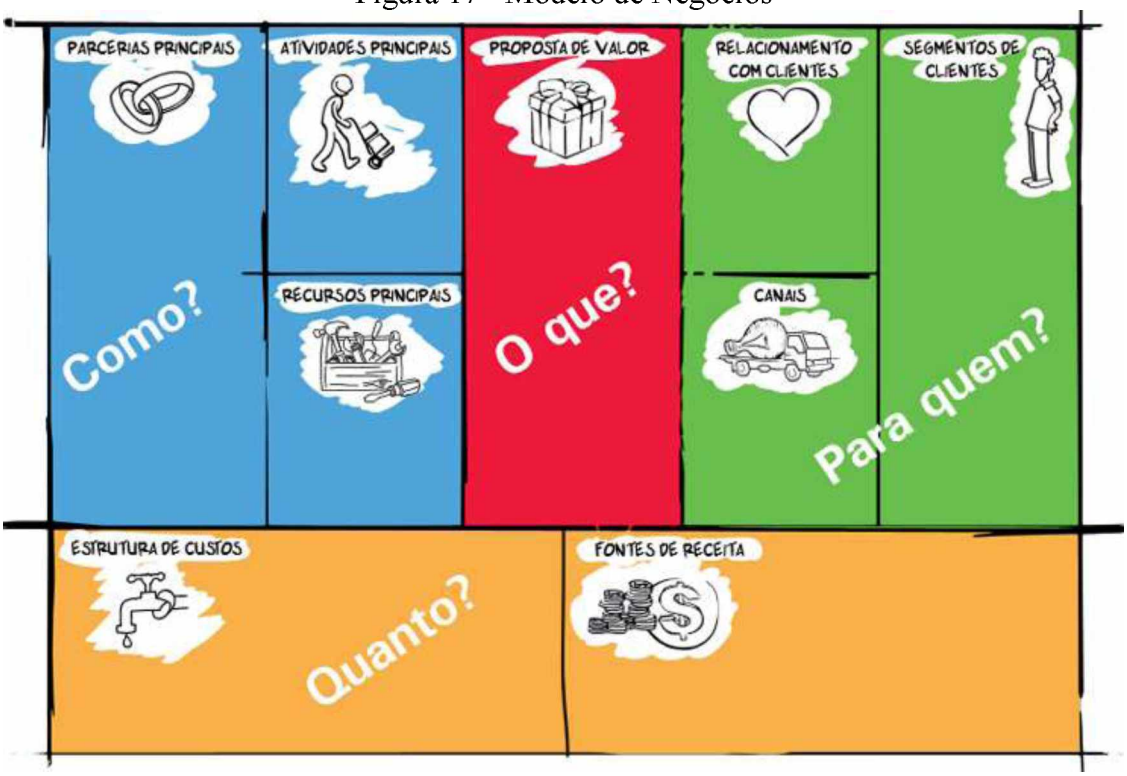
4.1 *Business Model* Canvas

O Quadro de Modelo de Negócios (*Business Model Canvas*) é uma ferramenta que serve para planejar e visualizar as principais funções de um negócio e suas relações. Ao fornecer uma visão holística e flexível do modelo de negócios, esse instrumento auxilia os empreendedores nos processos de criação, diferenciação e inovação, fornecendo uma visão mais ampliada daquilo que o negócio abrangerá.

Quatro etapas básicas compõem essa estrutura: o que, quem, como e quanto. Elas de dividem em nove blocos (ou funções) que devem ser preenchidos da maneira mais adequada e intuitiva para facilitar o acréscimo, a remoção e a realocação das ideias. É importante ressaltar que o Modelo de Negócios não é sinônimo de Plano de Negócios: a análise e reflexão sobre o Modelo possibilitam a elaboração de um Plano bem estruturado e com maior potencial de sucesso. Mudanças no Modelo de Negócios implicam automaticamente atualizações no Plano de Negócios.

Com a ajuda desse quadro o empreendedor cria o seu Modelo de Negócios com quatro conceitos que fazem muita diferença (SEBRAE, 2015): pensamento visual, visão sistêmica, cocriação, e simplicidade e aplicabilidade (Figura 17).

Figura 17 - Modelo de Negócios



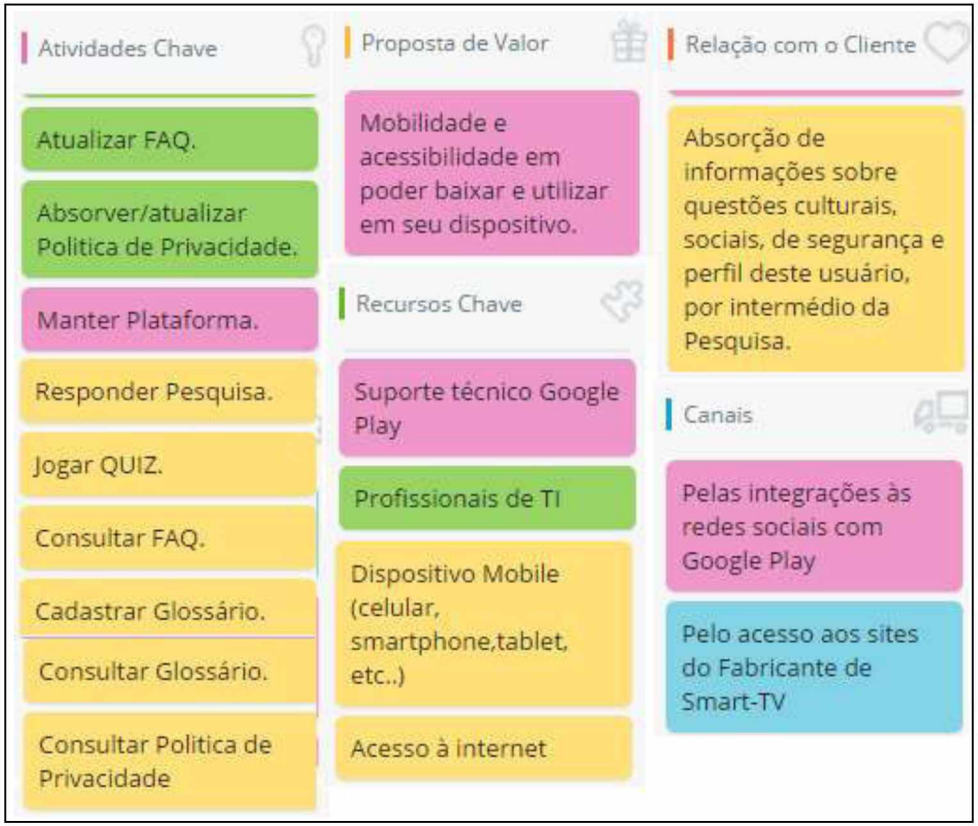
Fonte: Sebrae (2015)

Com base em toda a flexibilidade, relevância e organização sistêmica e mental proporcionada pelo Modelo Canvas, aplicou-se a ferramenta/quadro ao plano de aplicação a ser criado, como se pode observar na Figura 18.

O fato de o Canvas trazer uma espécie de mapa visual que apresenta uma estrutura fixa a ser preenchida visando ao planejamento, à reflexão ou mesmo à facilitação da visualização de alguma situação específica faz com que seu modelo seja bastante agregador do ponto de vista das tomadas de decisão. Entre as vantagens de se utilizar o Canvas está a velocidade de construção/preenchimento, as facilidades de comunicação, além da garantia de que há uma relação entre o preenchimento dos blocos que o compõem, uma vez que eles estão lado a lado na mesma página. Os modelos Canvas têm se mostrado muito eficientes em função da simplicidade na elaboração e entendimento dos conceitos, além de servirem de excelente ferramenta de comunicação e controle na implementação de um modelo de negócio, seja a nível de serviço ou produto.

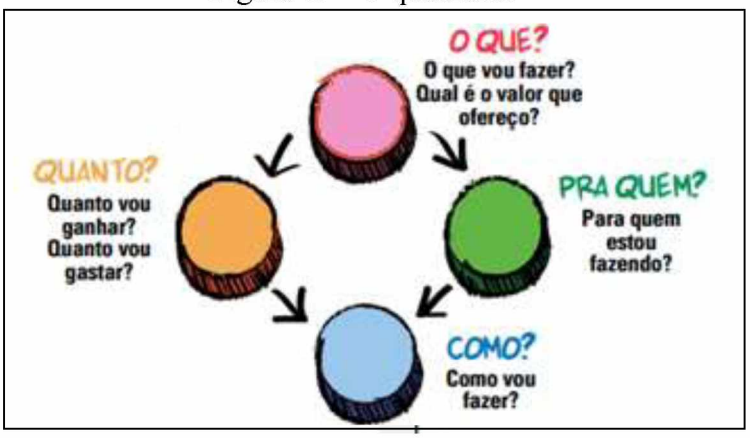
Figura 18 - Plano de aplicação segundo o Modelo Canvas

Continuidade da Figura 18:



Fonte: Peixoto (2015).

Figura 19 - O quadrante



Fonte: Elaborado pelo autor.

O uso das cores ajuda a identificar melhor toda a distribuição relacionada ao parceiro-chave, às atividades, às propostas de valor, à relação com cliente, aos segmentos de mercado, aos recursos, aos canais, às estruturas de custo e às fontes de renda, demonstrando que existe toda uma relação dos diferentes silos para com as cores, sendo que a rosa representa aquilo que vou fazer e o valor que ofereço, a verde para quem estou fazendo, a azul como vou realizar minha proposta, e a cor laranja, quanto vou ganhar e gastar.

4.2 Matriz SWOT

A análise SWOT (análise de **F**orças, **O**portunidades, **F**raquezas e **A**meaças - FOFA) é uma estrutura para identificar e analisar os fatores internos e externos que podem ter impacto sobre a viabilidade de um projeto, produto, lugar ou pessoa.

O quadro gerado pela análise SWOT é creditado a Albert Humphrey, que testou a abordagem em 1960 e 1970 no Instituto de Pesquisas de Stanford. Desenvolvida para negócios e baseada em dados empresariais, a análise SWOT tem sido adotada por organizações de todos os tipos como uma ajuda para a tomada de decisões.

Como seu nome indica, uma análise SWOT examina quatro elementos:

a) **Fortalezas**: atributos internos e recursos que suportam um resultado bem-sucedido.

b) **Oportunidades**: fatores externos que o projeto possa capitalizar ou usar para sua vantagem

c) **Fraquezas**: recursos ou atributos internos que trabalham contra um resultado de sucesso.

d) **Ameaças**: fatores externos que possam comprometer o projeto.

Uma vez que os fatores da SWOT sejam identificados, os tomadores de decisão devem ser capazes de melhor verificar se o projeto ou objetivo vale a pena e aquilo que será necessário para torná-lo bem-sucedido.

Define-se então qual tipo de estratégia será a mais adequada, tendo em vista a sua capacitação e o objetivo estabelecido. Entretanto, é preciso estar ciente de que a escolha norteará os rumos do projeto por um período de tempo que poderá ser longo em alguns casos.

As estratégias estabelecidas podem estar voltadas à **sobrevivência**, à **manutenção**, ao **crescimento** ou o **desenvolvimento**, conforme a situação ou postura estratégica da empresa. A combinação de estratégias deverá ser realizada no momento certo e feita de forma a que se aproveitem todas as oportunidades possíveis. A Figura 20 apresenta a análise do produto em questão nas quatro vertentes citadas anteriormente.

Figura 20 - Cálculo da Matriz SWOT para o COSI

Análise SWOT - C.O.S.I			
Fatores	Nota (1-5)	Fatores	Notas (1-5)
Análise Interna			
Fortalezas (Strengths)		Fraquezas (**W**eaknesses)	
Único lugar onde se encontram centralizadas as Pol.de Privacidade	5,0	Depende de um administrador para atualizar informações e gerar nova versão	5,0
Oferece versão gratuita do aplicativo	5,0	Aplicativo compatível apenas com sistema operacional Android	4,0
Local confiável em poder baixar o aplicativo (Google Play)	3,0	Baixa adesão inicial em função do foco ser voltado para categoria de TV tipo Smart	4,0
Mobilidade em poder utilizar no celular / smartphone	4,0	Utilização prévia somente na pré-compra/adquisição da Smart-TV, não usando tanto no pós.	3,5
Produto colaborativo, educativo e instrutivo	4,5	Dificuldade em localização do aplicativo pela grande quantidade de aplicativos (Google Play)	1,0
Gera conhecimentos sobre segurança das informações	4,0	Dependencia de estar online para usufruir de alguns dos recursos	2,0
Média	4,3	Média	3,8
Análise Externa			
Oportunidades (**O**pportunities)		Ameaças (**T**hreats)	
Segmento Smart-TV em crescimento, além de meio de comum. de massa	4,0	Mudanças constantes do link/URL das politicas de priv do fabricante ou dificuldades em achar	4,0
Expansão e integração com redes sociais como gestão do conhecimento	2,5	Por questões culturais, baixo conhecimento e conscientização perante segurança das informac	5,0
Patrocinio de fabricantes de Smart-TV	3,5	Google Play estar indisponivel para baixar os aplicativos ou começar a cobrar de todos hospedad	2,5
Converter em um aplicativo pago (em caso de novas features)	4,0	Surgimento de aplicativos do mesmo genero ou similares	3,0
Com base na Pesquisa, fomentar novas condutas e praticas de Seg. junto ao Fabricante	3,5	Hardware do dispositivo mobile não suportar o aplicativo ou conflito com determinado modelo	2,0
Aumentar o nivel de conscientização do usuario-cliente perante a segurança das infor.	4,5	Inacessibilidade total da internet no pais	1,0
Média	3,8	Média	2,8

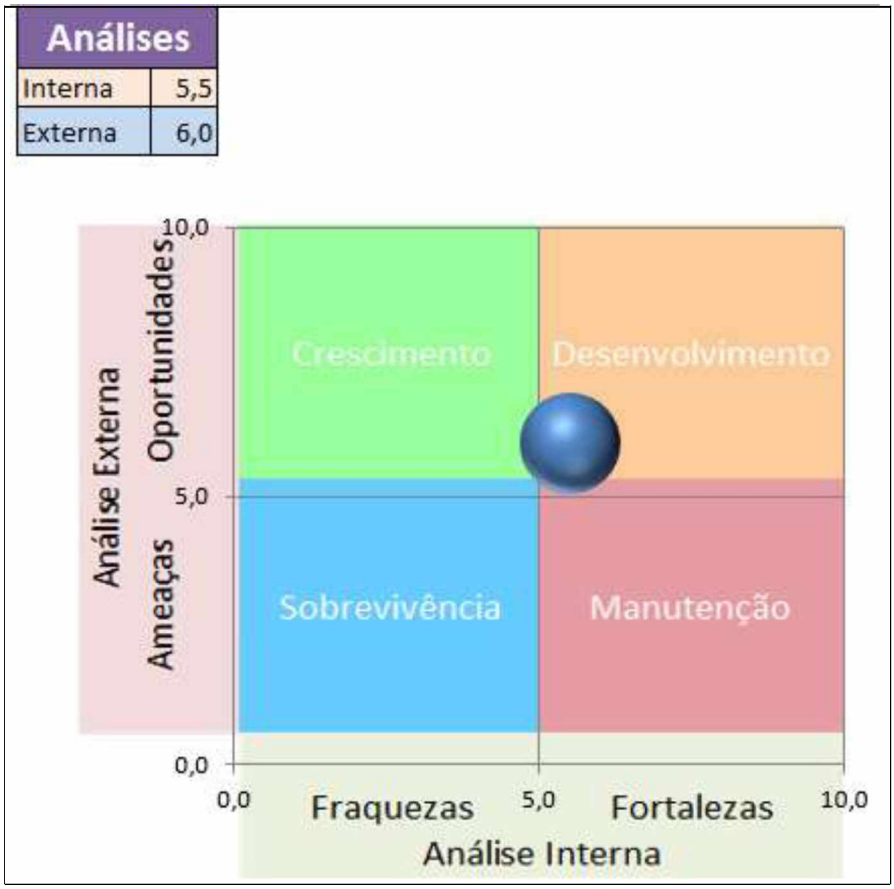
Fonte: Elaboração/preparação do próprio autor.

Conforme observado, foram aplicados os aspectos inerentes às situações/características do produto realizando-se a análise SWOT numa ferramenta/planilha que segue os critérios de avaliação para cada um dos quatro elementos (fortalezas, fraquezas, oportunidades e ameaças) para o empreendimento/aplicativo, conseguindo-se obter as seguintes médias:

- Fortalezas = 4.3
- Oportunidades = 3.8
- Fraquezas = 3.8
- Ameaças=2.8

Foram lançadas notas de 0 a 5 para cada situação/característica de cada elemento da SWOT, de forma que a ferramenta realiza o cálculo da média final com uma visão interna e externa para cada elemento.

Figura 21 - Análise interna e externa do posicionamento estratégico atual do COSI



Fonte: Elaboração/preparação do próprio autor.

Como se pode observar na Figura 21, o resultado da avaliação geral interna foi de 5,5 e, da visão externa, 6,0 (numa escala de 0 a 10). O dimensionador de ponderação tendeu para uma estratégia momentaneamente em "**desenvolvimento**", o que de certa forma faz sentido, pois sua situação é predominantemente empreendedora para os pontos **fortalezas** e **oportunidades**. Diante disso, deve-se procurar desenvolver o produto em duas direções: podem-se (se necessário) procurar novos mercados e clientes ou, então, tecnologias diferentes daquelas que se domina. A combinação dessas duas direções permite ao empreendedor construir novos negócios no mercado.

4.3 Matriz GUT

Embora não seja uma obrigatoriedade nem ao menos uma regra, tomar-se-ão aqui como premissa, na entrada dos problemas a serem tratados na Matriz GUT, os quesitos referentes às **fraquezas** e **ameaças** da Análise SWOT realizada no tópico anterior, sendo que as pontuações lançadas para cada item foram fruto exclusivo da análise do próprio autor deste trabalho com base em suas percepções e experiências.

A Matriz de Priorização de GUT (Gravidade x Urgência x Tendência) foi proposta por Charles H. Kepner e Benjamin B. Tregoe em 1981 como uma das ferramentas utilizadas na solução de problemas. Ela é uma ferramenta de qualidade usada para definir prioridades dadas às diversas alternativas de ação (COLENGHI,1997).

O objetivo dessa ferramenta é priorizar as ações de forma racional, levando em consideração a gravidade, a urgência e a tendência do fenômeno, permitindo escolher a tomada de ação menos prejudicial (KEPNER; TREGOE, 1991).

a) GRAVIDADE: intensidade, profundidade dos danos que o problema pode causar se não se atuar sobre ele.
b) URGÊNCIA: tempo para a eclosão dos danos ou resultados indesejáveis se não se atuar sobre o problema.
c) TENDÊNCIA: desenvolvimento que o problema terá na ausência de ação.

Essa ferramenta responde racionalmente às questões:

a) O que devemos fazer primeiro?
b) Por quê?
c) Por onde devemos começar?

Etapas:

a) listar os problemas ou os pontos de análise;
b) pontuar cada tópico;
c) classificar os problemas;
d) tomar decisões estratégicas.

Campos de análise:

GRAVIDADE

1 = SEM GRAVIDADE (dano mínimo)

2 = POUCO GRAVE (dano leve)

3 = GRAVE (dano regular)

4 = MUITO GRAVE (grande dano)

5 = EXTREMAMENTE GRAVE (dano gravíssimo)

URGÊNCIA

1 = Longuíssimo prazo (dois ou mais meses) - NÃO HÁ PRESSA

2 = Longo prazo (um mês) - PODE AGUARDAR

3 = Prazo médio (uma quinzena) - O MAIS CEDO POSSÍVEL

4 = Curto prazo (uma semana) - COM ALGUMA URGÊNCIA

5 = Imediatamente (está ocorrendo) - AÇÃO IMEDIATA

TENDÊNCIA

1 = Desaparece ou NÃO VAI PIORAR, PODENDO ATÉ MELHORAR

2 = Reduz-se ligeiramente ou VAI PIORAR EM LONGO PRAZO

3 = Permanece ou VAI PIORAR EM MÉDIO PRAZO

3= Aumenta ou VAI PIORAR EM POUCO TEMPO

5 = Piora muito ou VAI PIORAR RAPIDAMENTE

Figura 22 - Resultado GUT (prioridade)

PROBLEMA	Gravidade	Urgência	Tendência	Prioridade
Aplicativo compativel apenas com sistema operacional Android	4	5	4	13
Mudanças constantes do link/URL das politicas de priv do fabricante ou dificuldades em achar	5	5	2	12
Depende de um administrador para atualizar informações e gerar nova versão	3	4	3	10
Dependencia de estar online para usufruir de alguns dos recursos	3	3	3	9
Google Play estar indisponivel para baixar os aplicativos ou começar a cobrar de todos hospedados	4	3	2	9
Hardware do dispositivo mobile não suportar o aplicativo ou conflito com determinado modelo	4	3	1	8
Inacessibilidade total da internet no pais	4	3	1	8
Dificuldade em localização do aplicativo pela grande quantidade de aplicativos (Google Play)	1	2	3	6
Por questões culturais, baixo conhecimento e conscientização perante segurança das informacões	3	2	1	6
Utilização prévia somente na pré-compra/adquisição da Smart-TV, não usando tanto no pós.	2	1	2	5
Surgimento de aplicativos do mesmo genero ou similares	2	1	2	5
Baixa adesão inicial em função do foco ser voltado para categoria de TV tipo Smart	2	1	1	4

Fonte: Elaboração/preparação do próprio autor.

Respondendo às três perguntas supracitadas na Figura 22, teríamos:

a) **O que devemos fazer primeiro?**
   - Providenciar nova arquitetura de configuração e engenharia de compatibilidade para maior flexibilidade do aplicativo diante de outros tipos de sistemas operacionais de mercado, além do Android.

b) **Por quê?**
   - Porque ser compatível somente com o Android restringe a acessibilidade para outros usuários, além levar à de perda de espaço para outros possíveis concorrentes.

c) **Por onde devemos começar?**
   - Realizar uma evolução do *Software Development Kit* (SDK), bem como de sua plataforma de desenvolvimento.

Em suma, a Matriz GUT é uma matriz de priorização considerada uma ferramenta de gestão para identificar, observar, analisar e buscar soluções para os problemas e desafios em uma organização ou empreendimento. Essa matriz estabelece a priorização baseada nos fatores de gravidade, urgência e tendência e consiste em uma tabela de pontuação (vista anteriormente) onde se pode visualizar facilmente quais itens têm maior prioridade em relação aos demais (OLIVEIRA, 1992).

4.4 MATRIZ CEB

A matriz de priorização CEB pode ser utilizada para inúmeras finalidades, contando sempre com as vantagens de possuir uma aplicação fácil. Ela com certeza auxilia a priorizar as ações a serem executadas com base no custo/benefício para acabar com diversos problemas em qualquer empresa/empreendimento. No nosso caso, nós a utilizamos com o intuito de priorizar o que de melhor temos no cenário para o produto/aplicação em questão, tomando-se como base novamente a Análise SWOT, agora nos quesitos referentes às **forças** e **oportunidades**. Novamente as pontuações lançadas para cada item foram de análise única do autor deste trabalho, e realizadas com base em suas percepções e experiências.

A matriz CEB utiliza os seguintes critérios de priorização:

- **C** – Custo: Quanto vai custar para implementar o produto (vamos ter que desembolsar dinheiro)? Quanto menor o custo, melhor.

- **E** – Esforço: Nível de esforço necessário para implementar o produto (vamos ter que nos dedicar). Quanto menor o esforço, melhor.
- **B** – Benefícios: Quanto vamos receber ao implementar o produto (vamos ter retorno)? Quanto maior o retorno, melhor.

A grande vantagem de utilizar a Matriz CEB é que ela auxilia o gestor a avaliar de forma quantitativa os problemas da empresa, tornando possível priorizar ações corretivas e preventivas para solucionar total ou parcialmente o problema. As aplicações e a utilização da matriz CEB são fáceis, e explicadas detalhadamente pela Arruda Consult (2015):

a) liste problemas, atividades, processos, ideias, soluções ou projetos com dificuldade de sequenciação;
b) classifique toda a lista conforme critérios de priorização (1, 3, 5, 7 e 9) em cada um dos fatores CEB;
c) a coluna "Peso (CxExB)" traz resultados automáticos com base na multiplicação das notas de cada um dos fatores CEB;
d) a coluna "% de Criticidade" também é automática e calcula os valores obtidos para cada problema, estabelecendo a maior relevância entre os itens da lista;
e) por fim, visualize os itens de maior relevância e trace um plano de ação para monitoramento e implementação dos que forem priorizados.

Figura 23 - Resultado da Matriz CEB (criticidade)

Lista de itens obtidos para priorização	C	E	B	Peso (CxExB)	% Criticidade
Converter em um aplicativo pago (em caso de novas features)	9	9	9	729	19%
Oferecer versão gratuita do aplicativo	9	7	9	567	15%
Possuir Mobilidade em poder utilizar no celular / smartphone	9	9	7	567	15%
Com base na Pesquisa, fomentar novas condutas e praticas de Seg. junto ao Fabricante	9	9	7	567	15%
Ser Único lugar onde se encontram centralizadas as Pol.de Privacidade	9	5	9	405	11%
Ser um Produto colaborativo, educativo e instrutivo	7	7	7	343	9%
Gerar conhecimentos sobre segurança das informações	7	5	9	315	8%
Patrocinio de fabricantes de Smart-TV	7	5	9	315	8%
Ser Local confiável em poder baixar o aplicativo (Google Play)	7	5	7	245	6%
Prevalecer como Segmento Smart-TV em crescimento, além de meio de comum. de massa	3	7	9	189	5%
Promover a Expansão e integração com redes sociais como gestão do conhecimento	5	5	7	175	5%
Aumentar o nivel de conscientização do usuario-cliente perante a segurança das infor.	5	3	9	135	4%

Fonte: Elaboração/preparação do próprio autor.

Com base nos resultados apresentados nos cálculos da CEB (Figura 23), podemos interpretar que o grau de criticidade mais alto para que haja um foco maior na atuação em termos de ações para melhor custo/benefício foi de 19%, referente a "converter em um aplicativo pago", o que faz sentido quando se leva em consideração uma visão consumista e de ganho de capital para gerar receita. Em seguida temos "oferecer versão gratuita do aplicativo", com 15%, que considera o lado de responsabilidade social e colaborativismo do produto. Com o mesmo percentual, 15%, "possuir mobilidade em poder utilizar no smartphone/celular" tem um peso forte também em função de ser um produto *out of the box*, possibilitando uma maior condição de ser baixado e utilizado com maior acessibilidade em diferentes aparelhos móveis.

Outro item com forte grau de criticidade, também com 15%, foi "com base na pesquisa, fomentar novas condutas e práticas de segurança junto ao fabricante", o que também faz sentido, pois um dos intuitos principais do produto em questão é fornecer possibilidade de conhecimento sobre as melhores práticas de segurança das informações com a interação entre cliente e fornecedor. Por isso, dentro do próprio aplicativo existe o recurso de poder participar da pesquisa, que pode ser respondida on-line. Outro item de alto grau de criticidade para que se mantenha o foco em questão, com 11%, foi "ser o único lugar onde se encontram centralizadas as políticas de privacidade". Esse é um item bastante importante e coerente, constituindo-se num dos principais pilares de contribuição deste estudo, pois as avaliações das políticas existentes de cada fabricante de Smart TV facilitam muito a vida do usuário, que em um único lugar pode consultar e esclarecer suas dúvidas sobre privacidade

5 MÉTODOS E TÉCNICAS

Na pesquisa descritiva realiza-se o estudo, a análise, o registro e a interpretação dos fatos do mundo físico sem a interferência do pesquisador. São exemplos de pesquisa descritiva as pesquisas mercadológicas e de opinião (BARROS; LEHFELD, 2007).

O processo descritivo visa à identificação, ao registro e à análise das características, fatores ou variáveis que se relacionam com o fenômeno ou processo. Esse tipo de pesquisa pode ser entendido como um estudo de caso em que, após a coleta de dados, é realizada uma análise das relações entre as variáveis para uma posterior determinação dos efeitos resultantes em uma empresa, sistema de produção ou produto (PEROVANO, 2014).

A pesquisa descritiva pode aparecer sob diversos tipos: documental, estudos de campo, levantamentos etc. As pesquisas quantitativas de descrição são mais bem conhecidas como pesquisas de levantamento de dados, de **sondagem** ou **survey**, e consistem na solicitação de informações a um grupo estatisticamente significativo de pessoas para posterior análise quantitativa, recorrendo-se a técnicas de pesquisa de campo.

No estudo em questão, esse processo englobou levantamentos bibliográficos e documentais pertinentes ao tema, observação direta e análise de informações e documentos apresentados por meio de análise de perfil do usuário/cliente utilizador do recurso tecnológico chamado Smart TV, bem como o levantamento da política de privacidade existente em alguns fabricantes de televisores. A pesquisa bibliográfica foi responsável por fornecer subsídios para uma melhor compreensão das temáticas abordadas na pesquisa ao serem analisados livros, revistas e artigos científicos e mercadológicos que tratam das políticas de privacidade no contexto da segurança das informações que transitam em equipamentos eletroeletrônicos, no caso, as televisões inteligentes – Smart TVs. Esse levantamento permitiu entender melhor se os fabricantes de fato se preocupam com a segurança das informações de seus usuários e se o usuário/cliente possui conscientização a respeito da vulnerabilidade desse equipamento no que se refere justamente à segurança dos seus dados pessoais.

A pesquisa exploratória foi essencial para o desenvolvimento deste plano de trabalho, uma vez que permitiu uma abordagem de entendimento mais prático e direto do que tem sido atualmente divulgado em termos de políticas de privacidade por cada fabricante de Smart TV no Brasil. Assim, foi possível saber quais fabricantes tiveram o trabalho de elaborar e divulgar tais políticas e ter também uma noção se, de fato, têm sido construídas políticas que respeitem o "cliente-consumidor".

A fim de se conhecer o significado que os sujeitos atribuem ao tema em questão, os dados descritivos deste estudo foram coletados por meio de pesquisa on-line (ex: *surveys*). Essa técnica de coleta de dados seguiu um formulário pré-definido com foco no usuário/cliente, com foco na natureza de sondagem (que variaram de 50 a 500 participantes), bem como enviados para profissionais de diversos segmentos na rede de relacionamentos Linkedin.

As questões do questionário foram elaboradas tendo por base a hipótese deste trabalho, trazendo, consequentemente, as percepções necessárias, como a detecção do perfil do usuário-telespectador de Smart TV, seus hábitos, cultura e atitudes que envolvem o contexto da privacidade e segurança das informações, seja no meio doméstico ou empresarial.

Para analisar os diferentes perfis absorvidos no processo de coleta de dados, tanto no universo dos grupos de discussão quanto em relação aos inúmeros integrantes do Linkedin na pesquisa, o presente trabalho fundamentou-se na Teoria da Informação, segundo a qual a informação é considerada um elemento objetivo da realidade exterior (CAPURRO, 1992 apud SIRIHAL; LOURENÇO, 2002, p. 4).

Para conhecer as ações dos atores em seu contexto natural, seu ponto de vista e sua perspectiva, Chizzotti (2005, p. 90, grifo do autor) defende a observação por meio do contato do pesquisador com o fenômeno observado.

> A observação direta pode visar uma *descrição* "fina" dos componentes de uma situação: os sujeitos em seus aspectos pessoais e particulares, o local e suas circunstâncias, o tempo e suas variações, as ações e suas significações, os conflitos e a sintonia de relações interpessoais e sociais, e as atitudes e os comportamentos diante da realidade.

Tal observação, por mais que não venha a ser *in loco*, desperta o mesmo nível de atenção ou até maior, pois a sensibilização diante das perguntas desenvolvidas deve ser rigorosamente considerada como fator preponderante em relação aos resultados de coleta. Por isso, mais importante ainda do que ser ou não presencial, é saber onde se quer chegar. Sendo assim, neste trabalho temos claramente o foco direcionado para os dois agentes principais desse contexto: o cliente/usuário e o fabricante. Nossa pretensão foi a de deixar claro se o fabricante leva em consideração a relação com seu cliente-usuário tendo por base o que consta em sua política de privacidade e se ela possui um foco mais de proteção do usuário ou só mercadológico, de negócio. E, por outro lado, buscou-se também o perfil do usuário-cliente de Smart TV, seja em âmbito domiciliar ou corporativo.

Concordamos com Goldenberg (2002, p. 14), que sintetiza seu pensamento da seguinte forma: "o que determina como trabalhar é o problema que se quer trabalhar: só se escolhe o caminho quando se sabe onde se quer chegar".

É importante lembrar ainda que a análise documental favorece a observação do processo de maturação ou de evolução de indivíduos, grupos, conceitos, conhecimentos, comportamentos, mentalidades, práticas, entre outros (CELLARD, 2008).

5.1 Pesquisa de sondagem

No que tange ao processo de coleta e análise de dados é importante introduzir o conceito de fluxo para uma melhor compreensão de toda essa cadeia até a chegada das tomadas de decisão perante um serviço, produto ou tendência.

Todo processo inicia-se com a coleta e composição dos dados. Em seguida estes são organizados de forma coerente, passando por uma etapa de análise em que se consegue compor informação, que por sua vez irá trazer o conhecimento, facilitando assim o processo de comunicação, que consequentemente conduzirá a uma tomada de decisão.

No entanto, faz-se necessária a definição do instrumento para a coleta dos dados, momento em que tudo se inicia. A seleção do instrumento depende do tipo de pesquisa, dos seus objetivos e também da teoria adotada como base para ela, de maneira a que os instrumentos forneçam dados de natureza qualitativa e quantitativa.

Para o nosso caso de pesquisa, algumas informações foram necessárias de antemão para um melhor entendimento de tudo o que foi coletado.

A pesquisa foi feita para a identificação e caracterização dos usuários de Smart TV, buscando uma melhor compreensão da forma como eles encaram a segurança de suas informações. Os dados coletados foram os de cadastro pessoal geral; dados sobre a cultura e os hábitos dos usuários de Smart TV; dados sobre segurança e orientação em âmbito técnico e de conhecimentos gerais do ambiente de TI. A melhor forma de coleta foi por intermédio de questionário com perguntas fechadas disponibilizado na Web. A pesquisa foi disponibilizada desta forma porque o público usuário de Smart TV é fluido, possui faixas etárias diversas e habita em diferentes lugares. Sendo assim, os dados foram coletados após a definição e formação do questionário elaborado, de acordo com o objetivo proposto neste trabalho, num período de 30 dias (de 1° de setembro a 1° de outubro de 2016), em formato on-line, tipo *survey*, pela ferramenta *Google Forms*.

Como a pesquisa teve o caráter de sondagem, não havendo a identificação dos respondentes, não foi necessário que ela fosse submetida ao Comitê de Ética (CEP), conforme Resolução nº 510, de 7 de abril de 2016 (Anexo A).

5.1.1 Público

A pesquisa foi realizada com um público de 109 pessoas de diferentes regiões, grande parte de Minas Gerais (76%), com idades que variavam entre 18 a 75 anos, sendo que a maior parte era de homens (74%) e tinha entre 25 e 35 anos (41,3%). A renda mensal média da maioria variou entre 4 e 6 salários mínimos (38%) e a maior parte (46,8%) era composta por pós-graduados, especialistas/MBA, sendo 48,6% da área de Tecnologia da Informação. Cerca de 77,1% trabalhavam em empresa privada, a grande maioria em tecnologia (28,4%) e educação (22,9%), e 53,2% dos entrevistados tinham filhos.

5.1.2 Cultura e hábitos

Grande parte do público pesquisado (71,6%) não possuía televisores mais antigos (do tipo tubo). O tempo médio que assistiam à TV por dia variava de 1 a 4 horas (63,3%), sendo que 55% possuíam apenas uma TV; e 36,7%, duas. Os fabricantes de Smart TV mais presentes nas casas/empresas eram: Samsung (52,3%), LG (40,4%) e Philips (15,6%). O tempo em que o entrevistado estava com a mesma fabricante de Smart TV variava de três a cinco anos (49,5%), sendo que os locais em que o usuário mais a utilizava eram a sala (88,1%) e o quarto (37,6%). Sua utilização era mais para acessar a internet (incluindo assistir à TV e a programas on-line), o que era feito por 70,6% dos respondentes, enquanto 62,4% se interessavam mais em assistir aos programas televisivos em geral (sobretudo os tradicionais da grade ou da TV a cabo/satélite). Já os recursos embutidos na Smart TV mais utilizados eram o HDMI (75,2%) e o Wi-Fi (69,7%).

5.1.3 Segurança

Com relação a ter acessado a internet por meio de sua Smart TV, cerca de 43,1% raramente tinham acessado e 38,5% acessavam com muita frequência. Sobre quem já tinha consultado/lido a política de privacidade de alguma Smart TV, 42,2% não haviam lido nem se preocupariam com isso mesmo sabendo que tal política existia. Dos entrevistados, 22,9% pré-

configuraram e testaram todos os detalhes no menu de configuração para som e imagem antes de ter a primeira experiência de uso com sua nova Smart TV. Quanto a ter se preocupado alguma vez com a segurança das informações que sua Smart TV pode absorver quando do cadastro de cliente/usuário ou na captura de imagem e som ou de dados em geral, cerca de 32,1% afirmaram ter pensado nisso mas nunca ter feito nada a respeito, e 30,3% não se preocuparam, pois desconheciam os riscos que estavam correndo. Com relação a quem realizou algum tipo de preenchimento de dados cadastrais ou informativos para cliente de Smart TV, 38,5% responderam que sim, como exigência do fabricante para poder usufruir de alguns recursos. Para 62,4%, uma política de privacidade de Smart TV serve para explicitar ao usuário que o fabricante terá o direito legítimo de recolher/captar informações, bem como para a explicação dos recursos existentes. Ao comprar uma Smart TV, 35,8% consideravam primordialmente o preço do aparelho, seu tamanho, a marca do fabricante e os cuidados com a segurança da informação do usuário. Cerca de 83,5% já tinham ouvido falar ou conheciam uma situação em que alguma Smart TV de um determinado fabricante havia comprometido a segurança das informações ou a privacidade de algum usuário-cliente. Para 16,5%, deveria ser possível existir algum recurso para "resetar" as configurações de sua Smart TV, sendo que alguns já tinham realizado esse procedimento pelo menos uma vez, e 25,7% não souberam responder a essa questão. Em termos de segurança das informações, priorizavam-se todos os elementos, confidencialidade, integridade e disponibilidade (55%), sendo que, dos três em questão, a confidencialidade era considerada o mais importante (33%). Para 40,4%, raramente costumava ocorrer problemas em sua Smart TV e, quando ocorria, rapidamente se estabilizava. Em termos de ociosidade perante sua Smart TV, o que mais acontecia era estar de frente para ela, mas sem estar atento ao que se passava (55%). Se a política de privacidade viesse anexada ao manual da Smart TV, 39,4% certamente iriam ler, e 32,1% achariam melhor se ela aparecesse ao se ligar pela primeira vez a TV. Sobre instalar algum novo *widget*, aplicativo, programa ou demais recursos em sua Smart TV, 40,4% instalariam somente os gratuitos. Para 57,8%, existia a preocupação periódica em checar se a última versão do *firmware* da Smart TV era a mais atual.

5.1.4 Orientação

Para 33,9%, se houvesse algum lugar onde se pudesse buscar facilmente orientações a respeito do que o fabricante poderia colher como informações por intermédio de sua Smart TV, seria justamente na política de privacidade, anexa ao manual impresso da TV, sendo que

para 30,3% seria melhor se tal orientação estivesse no *site* do próprio fabricante ou em outro *site* qualquer. Caso houvesse algum tipo de programa/aplicativo para celular que fizesse gratuitamente o download da política de privacidade, permitindo ao usuário consultar se determinado fabricante a possuía ou não antes de adquirir uma Smart TV, 45% certamente o utilizariam. Cerca de 83,5% nunca haviam entrado em contato com o suporte da fabricante para solucionar qualquer problema, e 58,7% tinham lido por completo o manual de sua Smart TV.

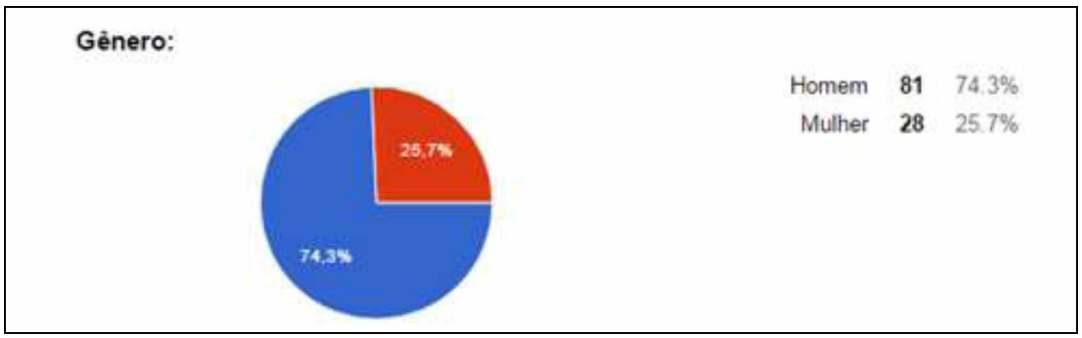
5.1.5 Geral

Cerca de 44% sabiam a que se refere a chamada "Internet das Coisas (IoT)", porém não a utilizavam. Já 31,2% nem sequer sabiam do que se tratava. Em torno de 45% não utilizava nenhum tipo de "Set Top Box (STB)", Dongle ou Media Box, porém 30,3% disseram utilizar. Para conseguir acessar a internet em sua Smart TV, 61,5% utilizavam a conexão nativa/embutida internamente (Wi-Fi), sendo que 19,3% utilizavam a conexão com fio (Porta Ethernet) ou via adaptador USB – Wi-Fi. Já 54,1%, antes de concretizar a compra de sua Smart TV na loja, não realizavam na prática testes de funcionalidade ou experimentação.

5.2 Análise dos resultados

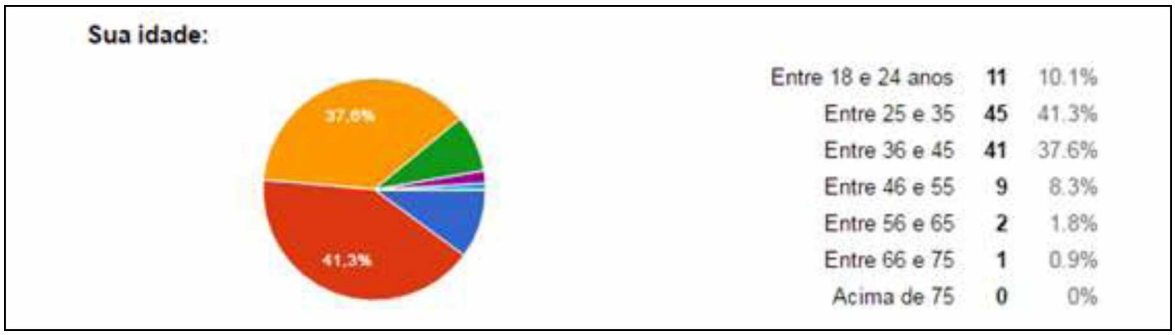
5.2.1 Público

Figura 24 - Sexo dos entrevistados



Fonte: Elaborado pelo autor.

Figura 25 - Idade dos entrevistados

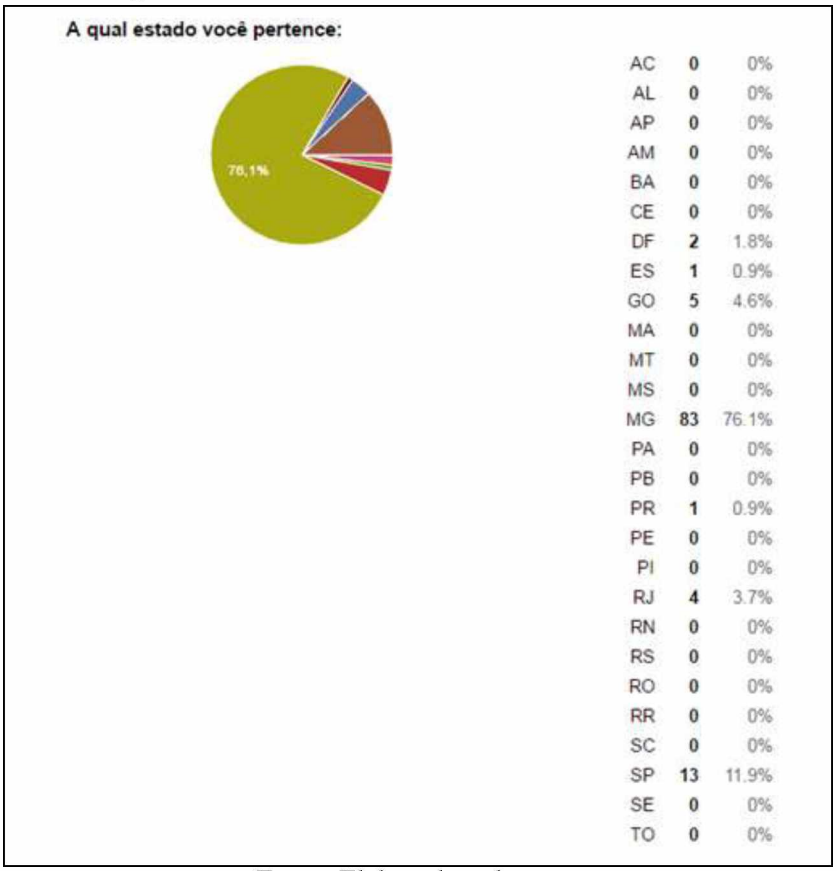


Fonte: Elaborado pelo autor.

Figura 26 - Renda dos entrevistados

Fonte: Elaborado pelo autor.

Figura 27 - Estado de residência dos entrevistados

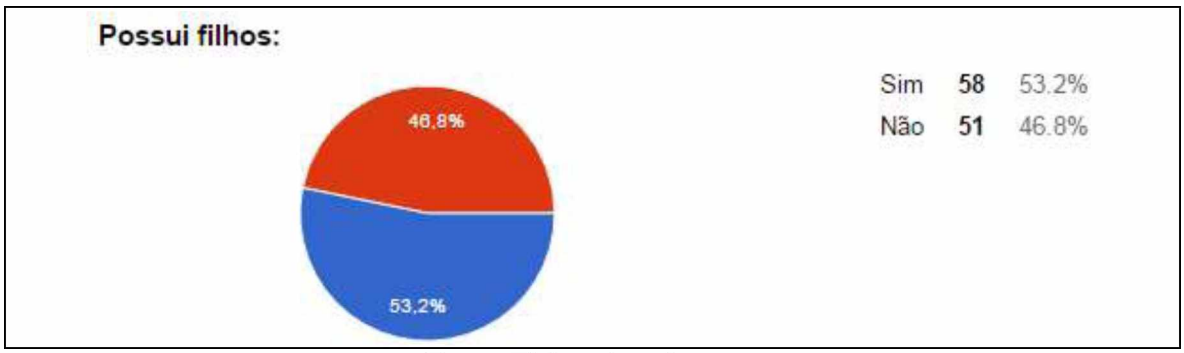


Fonte: Elaborado pelo autor.

Figura 28 - Escolaridade dos entrevistados

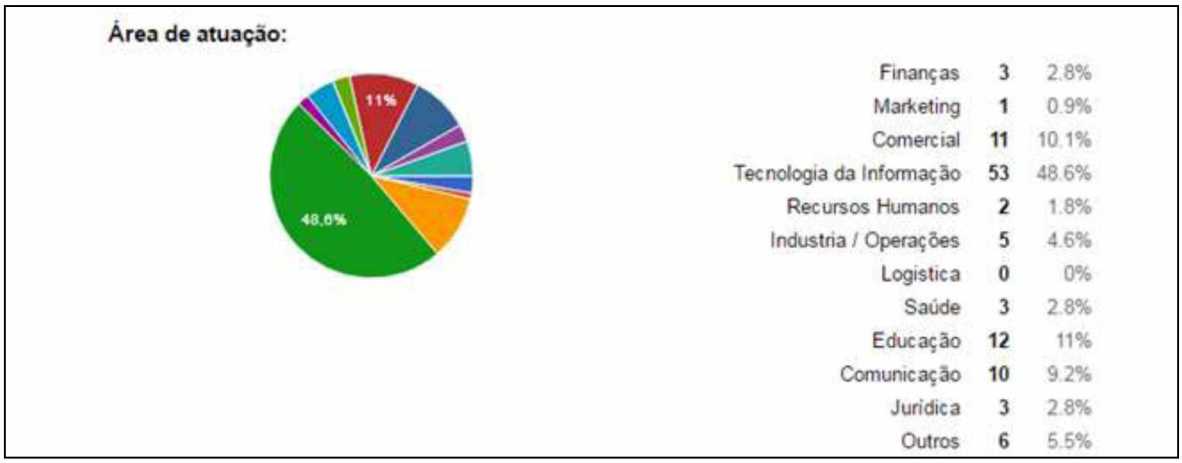
Fonte: Elaborado pelo autor.

Figura 29 - Quantidade de filhos dos entrevistados



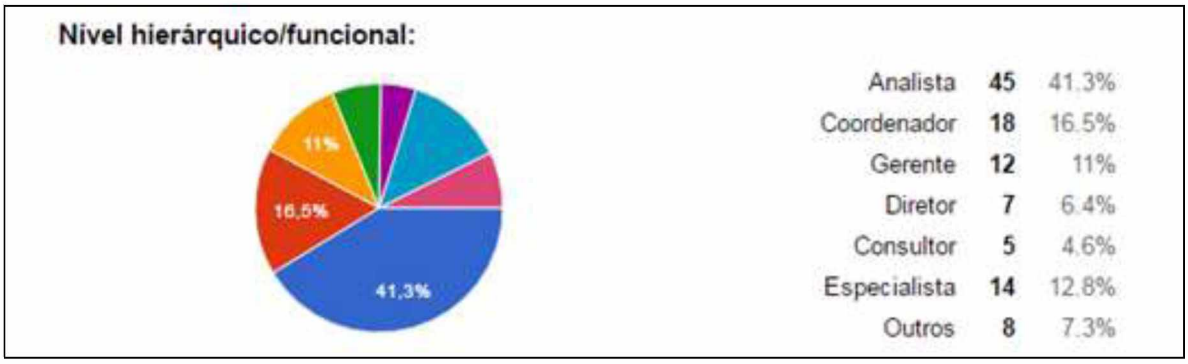
Fonte: Elaborado pelo autor.

Figura 30 - Segmento de atuação dos entrevistados



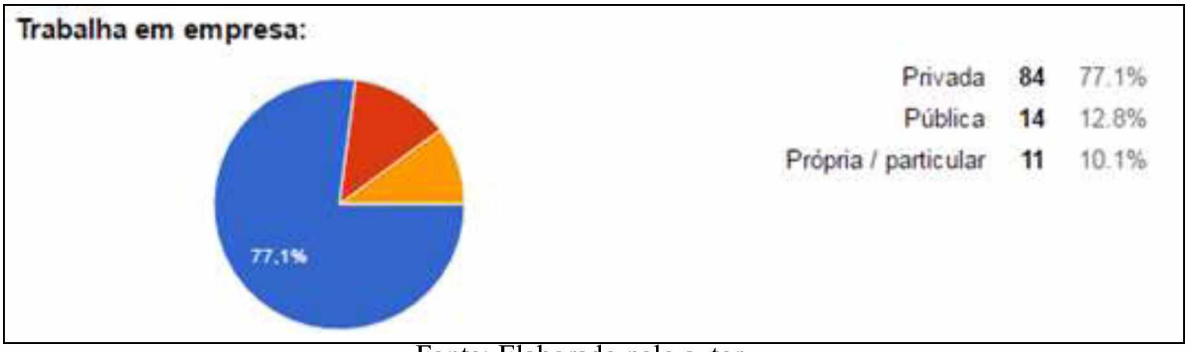
Fonte: Elaborado pelo autor.

Figura 31 - Função dos entrevistados



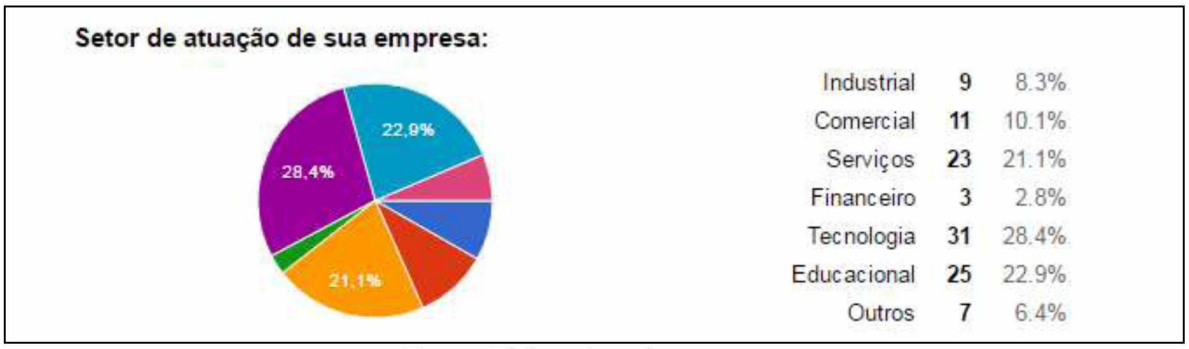
Fonte: Elaborado pelo autor.

Figura 32 - Empresa onde os entrevistados trabalham



Fonte: Elaborado pelo autor.

Figura 33 - Setor de atuação dos entrevistados

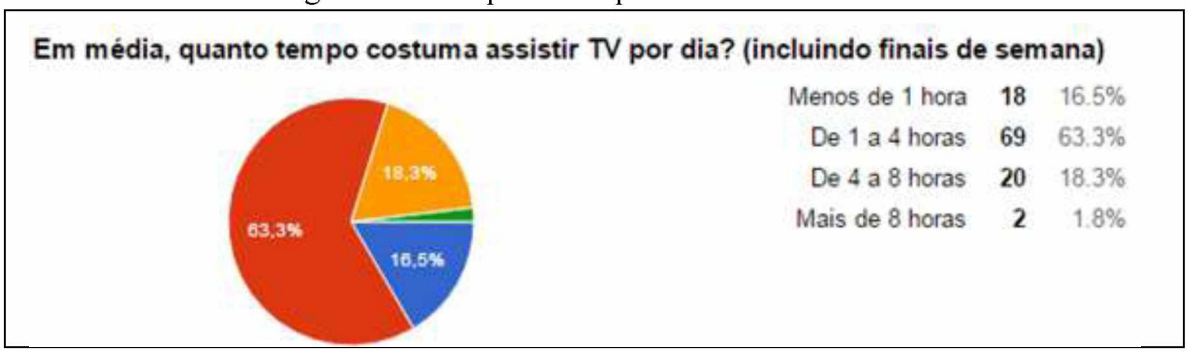


Fonte: Elaborado pelo autor.

Figura 34 - Tipo de TV dos entrevistados

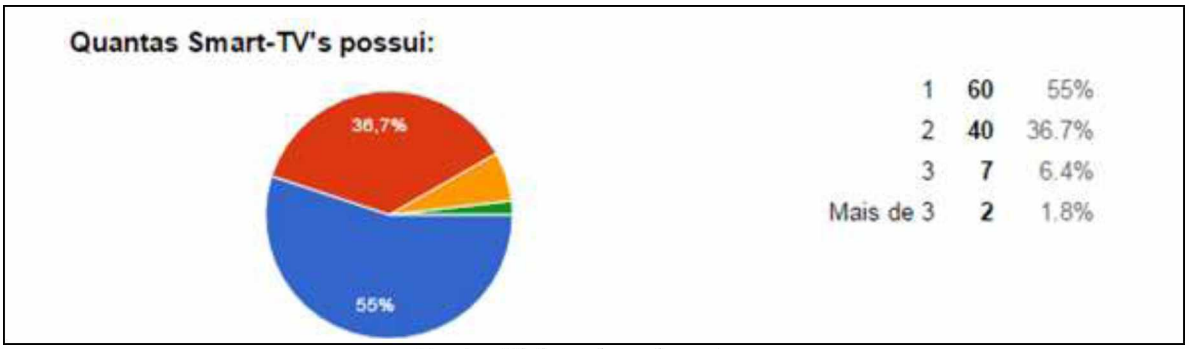
Fonte: Elaborado pelo autor.

Figura 35 - Tempo médio passado diante da TV



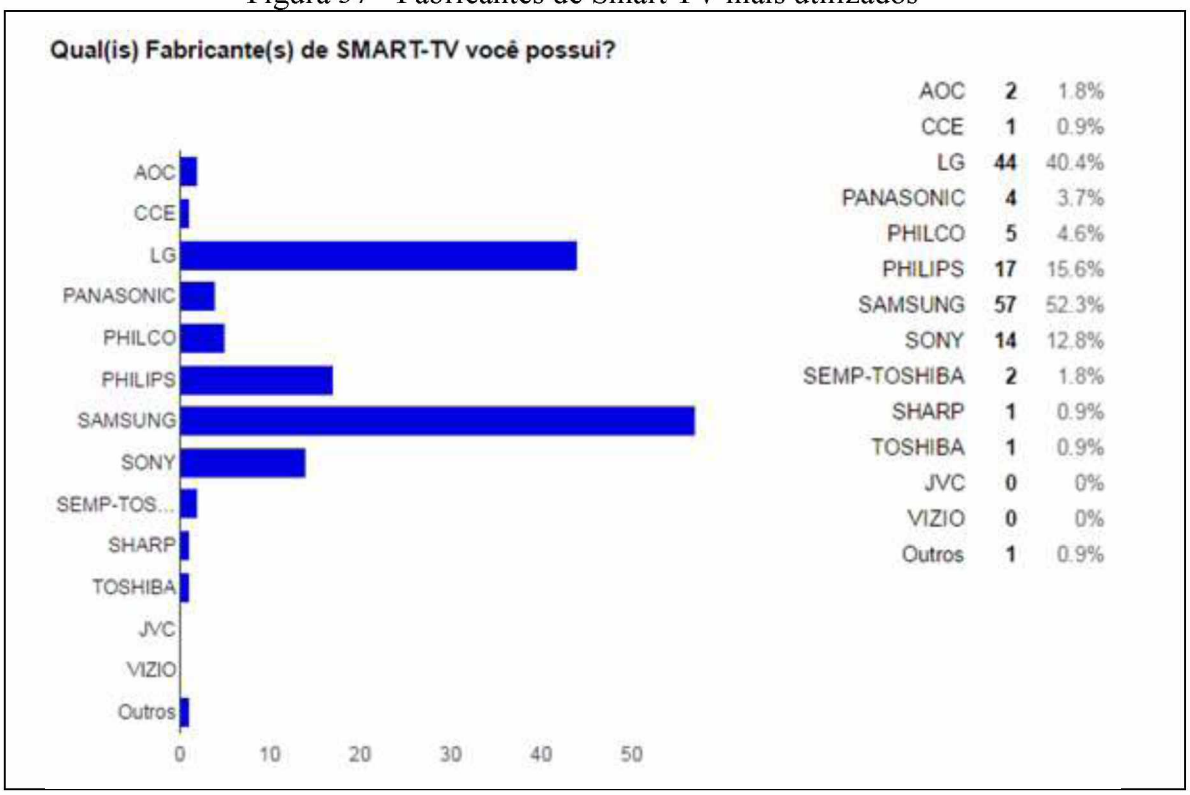
Fonte: Elaborado pelo autor.

Figura 36 - Quantidade de TVs dos entrevistados



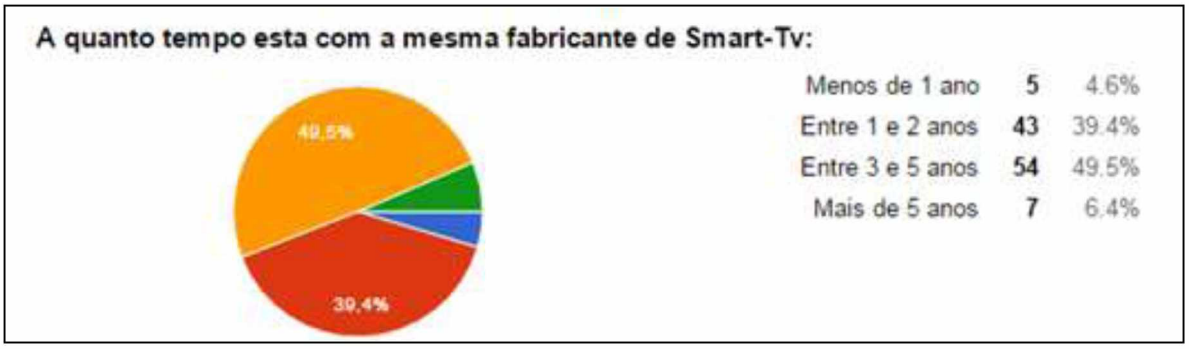
Fonte: Elaborado pelo autor.

Figura 37 - Fabricantes de Smart TV mais utilizados



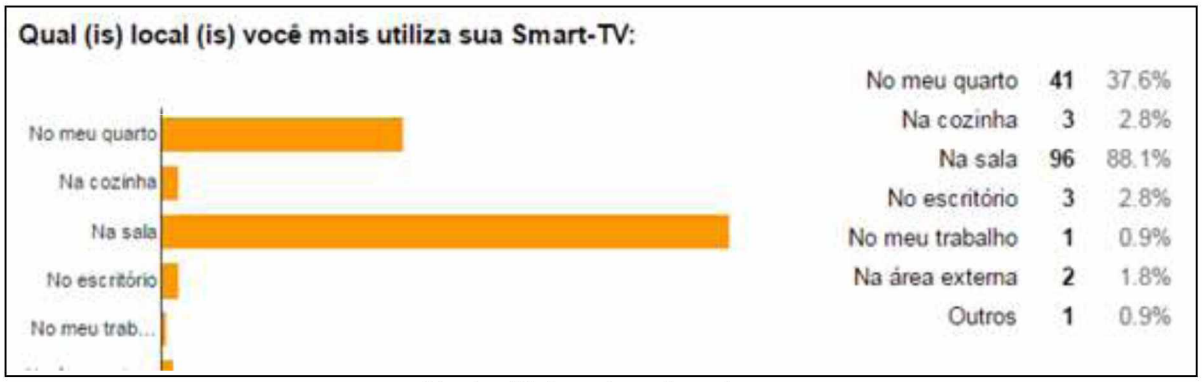
Fonte: Elaborado pelo autor.

Figura 38 - Tempo de permanência com o mesmo fabricante



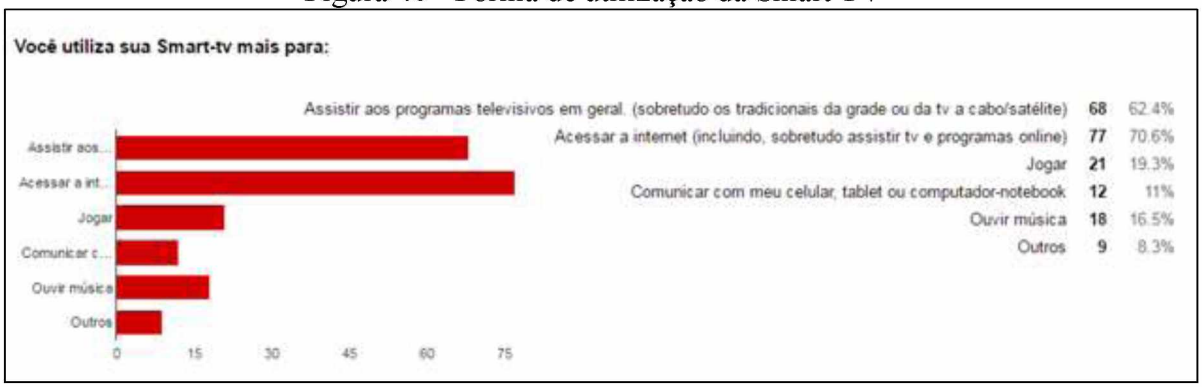
Fonte: Elaborado pelo autor.

Figura 39 - Local de utilização da Smart TV



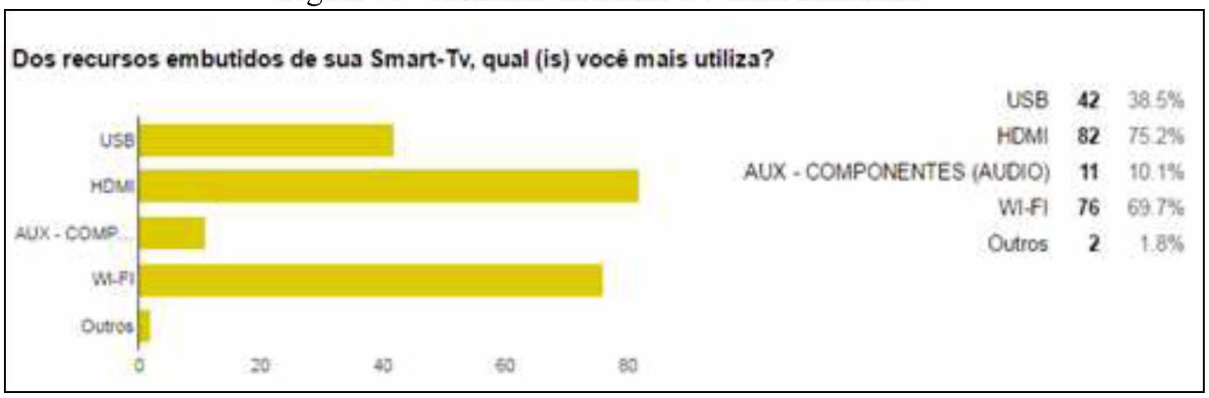
Fonte: Elaborado pelo autor.

Figura 40 - Forma de utilização da Smart TV



Fonte: Elaborado pelo autor.

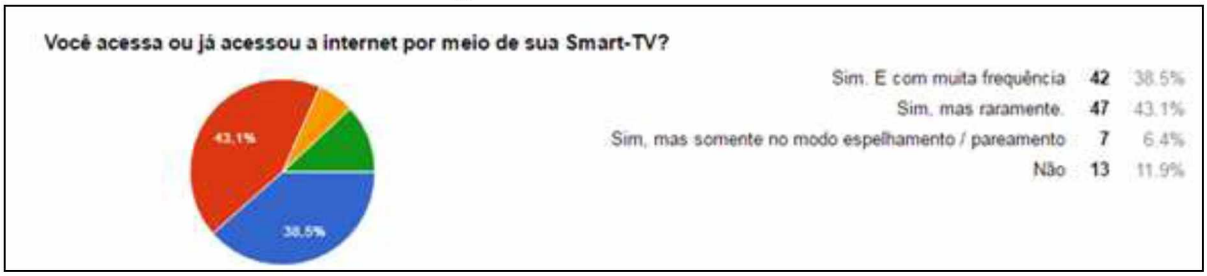
Figura 41 - Recursos da Smart TV mais utilizados



Fonte: Elaborado pelo autor.

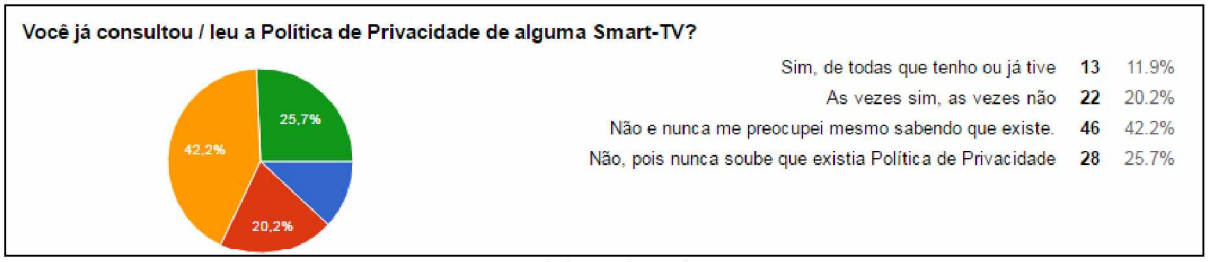
5.2.2 Segurança

Figura 42 - Acesso à internet



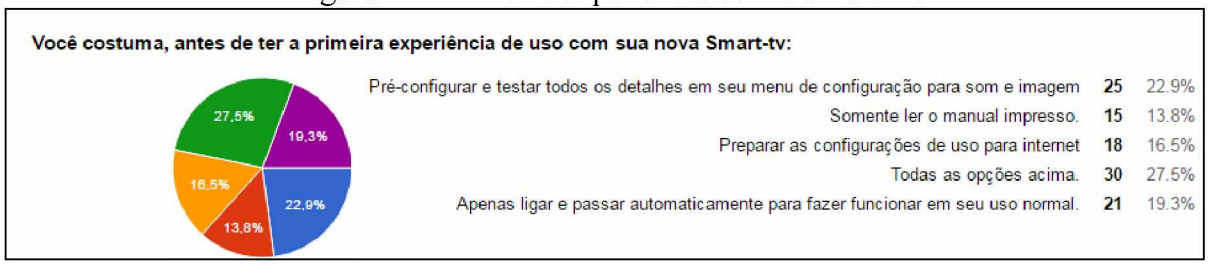
Fonte: Elaborado pelo autor.

Figura 43 - Política de privacidade da Smart TV



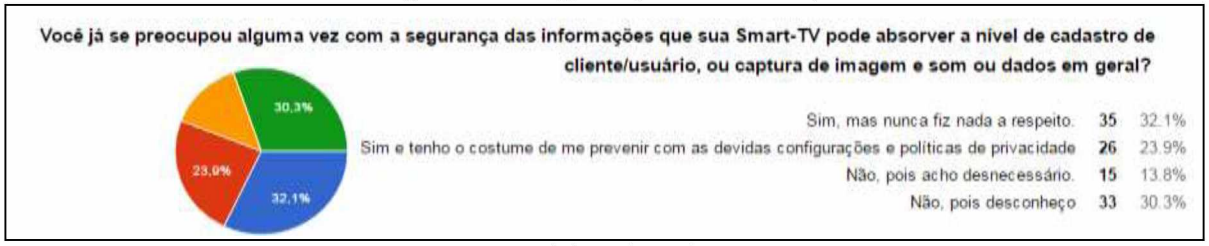
Fonte : Elaborado pelo autor.

Figura 44 - Primeira experiência com a Smart TV



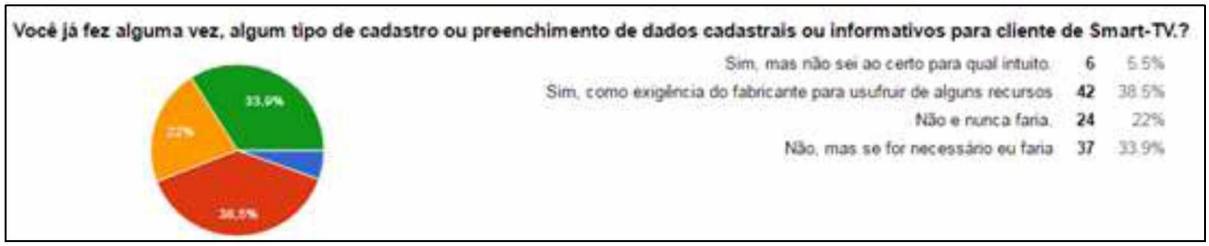
Fonte: Elaborado pelo autor.

Figura 45 - Segurança da informação



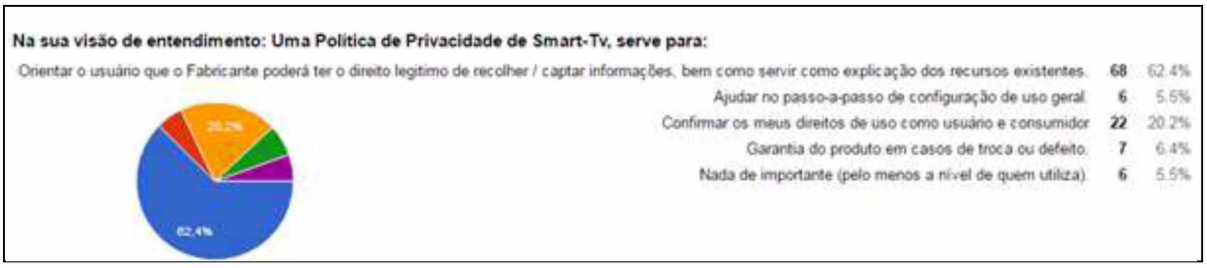
Fonte: Elaborado pelo autor.

Figura 46 - Cadastro para cliente de Smart TV



Fonte: Elaborado pelo autor.

Figura 47 - Utilidade da política de privacidade

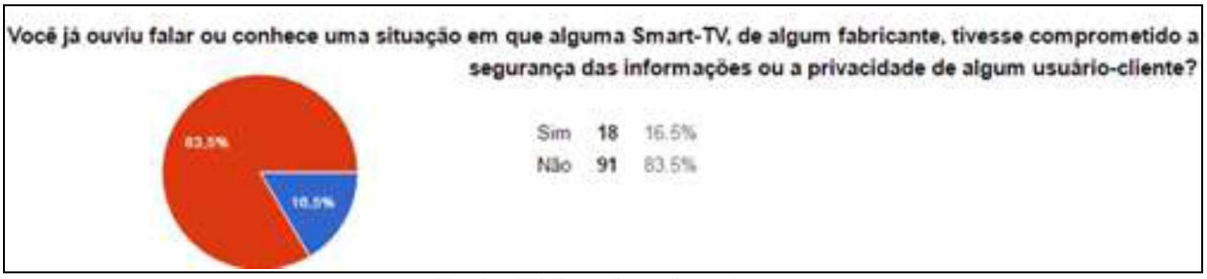


Fonte: Elaborado pelo autor.

Figura 48 - Requisitos para a compra de uma Smart TV

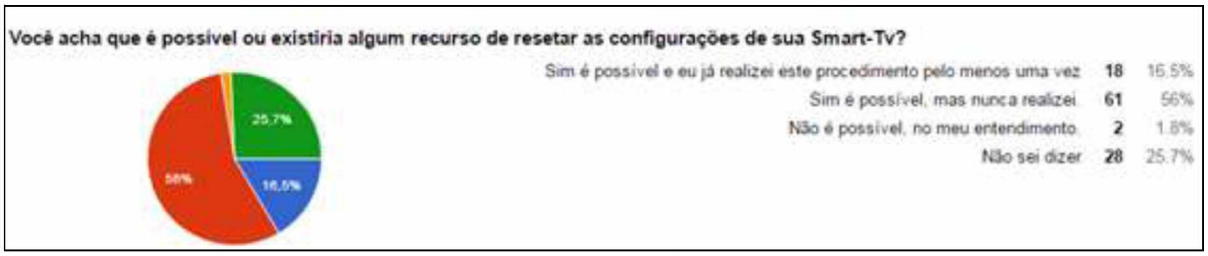
Fonte: Elaborado pelo autor.

Figura 49 - Comprometimento das informações



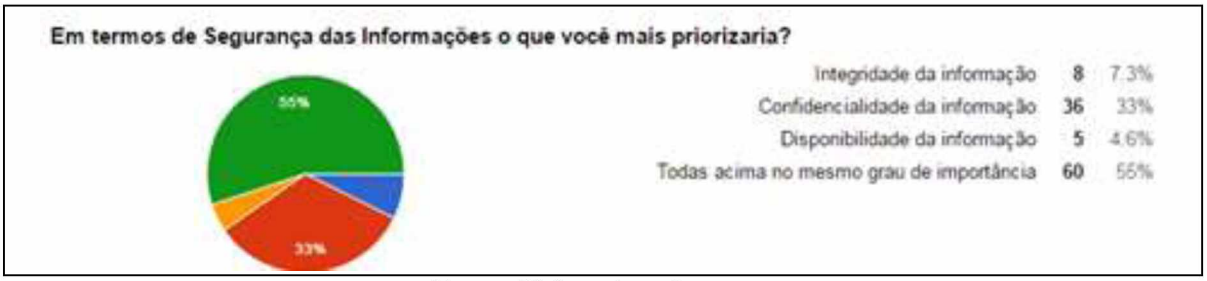
Fonte: Elaborado pelo autor.

Figura 50 - Configuração da Smart TV



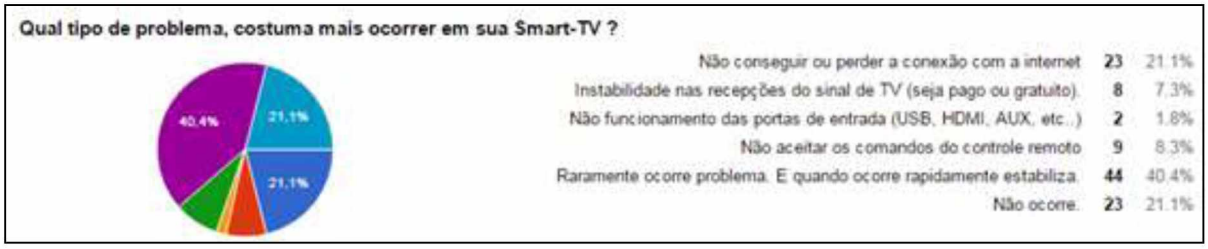
Fonte: Elaborado pelo autor.

Figura 51 - Prioridade de segurança das informações



Fonte: Elaborado pelo autor.

Figura 52 - Problemas com a Smart TV



Fonte: Elaborado pelo autor.

Podem-se tirar algumas conclusões interessantes com base nos resultados que foram colhidos. As classes média e alta são, por enquanto, as detentoras de uma fatia maior que utiliza as TVs inteligentes. Outra questão é o nível de escolaridade alto desse público e a

existência de uma certa fidelização em relação ao fabricante (até 5 anos). Como uma Smart TV apresenta inúmeras e diferentes possibilidades se comparada a um aparelho de televisão comum, de fato o usuário utiliza e explora muito os recursos on-line, fugindo do tradicional (grade televisiva), apesar de que o ato de navegar na internet por intermédio dela ainda é tímido. Uma informação que vale ressaltar é a quantidade de pessoas que, mesmo sabendo dos perigos de privacidade a que estão sujeitos os usuários de Smart TV, não toma nenhuma precaução ou cuidado com configurações e checagens. Isso sem contar os que ainda desconhecem por completo os perigos iminentes e reais, ou que sequer ouviram falar a respeito deles. Já os cuidados com a segurança das informações do usuário ainda não é prioridade para a grande maioria, sendo o preço o fator preponderante quando o usuário se decide a comprar uma Smart-TV. Existe ainda um certo interesse na leitura da política de privacidade, caso ela esteja mais facilmente disponível, por exemplo anexada ao próprio manual ou presente em um aplicativo mobile gratuito.

5.3 Descrição da plataforma de desenvolvimento

Para a realização deste projeto, a construção de um aplicativo para ambiente mobile, pretende-se utilizar a plataforma de programação orientada para eventos em celulares com sistema operacional Android, chamada MIT App Inventor 2.

O *App Inventor* é uma aplicação web de código aberto para Android originalmente fornecido pelo Google e agora mantido pelo Instituto de Tecnologia de Massachusetts (MIT). Ele permite criar aplicações de software para o sistema operacional Android por meio de uma interface gráfica que possibilita aos usuários arrastar e soltar objetos visuais para criar um aplicativo que possa ser executado em dispositivos Android.

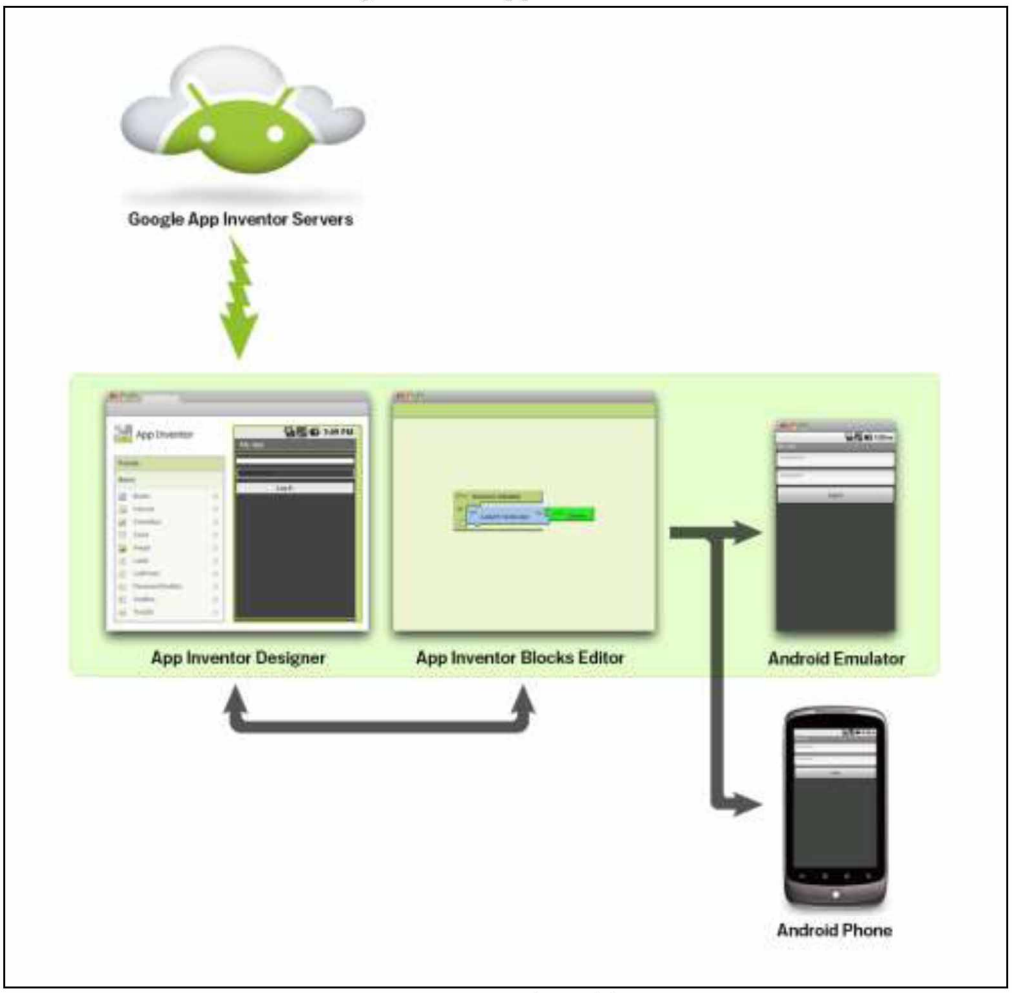
Ele se baseia na aprendizagem das teorias construcionistas, que salientam que a programação pode ser um veículo para propagar ideias poderosas por intermédio da aprendizagem ativa. Como tal, é parte de um movimento em curso em computadores e na educação que começou com o trabalho de *Seymour Papert* junto com o Grupo MIT na década de 1960, e também com *Mitchel Resnick,* no trabalho em *Lego Mindstorms e StarLogo* (HARDESTY, 2010).

O aplicativo foi disponibilizado em 12 de julho de 2010 e lançado publicamente em 15 de dezembro do mesmo ano. No segundo semestre de 2011, o Google lançou o código-fonte, rescindiu o seu servidor e forneceu o financiamento para a criação do *MIT Center for Mobile Learning*, liderado pelo criador do *App Inventor,* Hal Abelson, e por colegas professores do

MIT, Eric Klopfer e Mitchel Resnick. A versão no MIT foi lançada em março de 2012. Em 6 de dezembro de 2013 foi liberado o MIT App Inventor 2, que renomeou a versão original "App Inventor Classic". Atualmente o novo *App Inventor 2* (*Companion MIT EA2*) permite a depuração em tempo real dos dispositivos conectados via Wi-Fi, e não apenas via USB.

O App Inventor 2 permite que sejam desenvolvidos aplicativos para telefones Android usando um navegador da web ou um telefone ou emulador conectado (Figura 53). Os servidores *App Inventor* guardam o trabalho (em *cloud*, na nuvem) desenvolvido pelo usuário, ajudando-o a manter o controle de seus projetos.

Figura 53 - App Inventor 2



Fonte: MIT (2015b).

Desta maneira, podem ser criados aplicativos trabalhando-se com:

a) o *Designer Inventor* App, em que o usuário pode selecionar os componentes para sua aplicação;

b) o *App Inventor* Blocos do Editor, em que são montados os blocos de programa que especificam como os componentes devem se comportar. Assim o usuário monta programas visualmente, encaixando peças como se faz num quebra-cabeças.

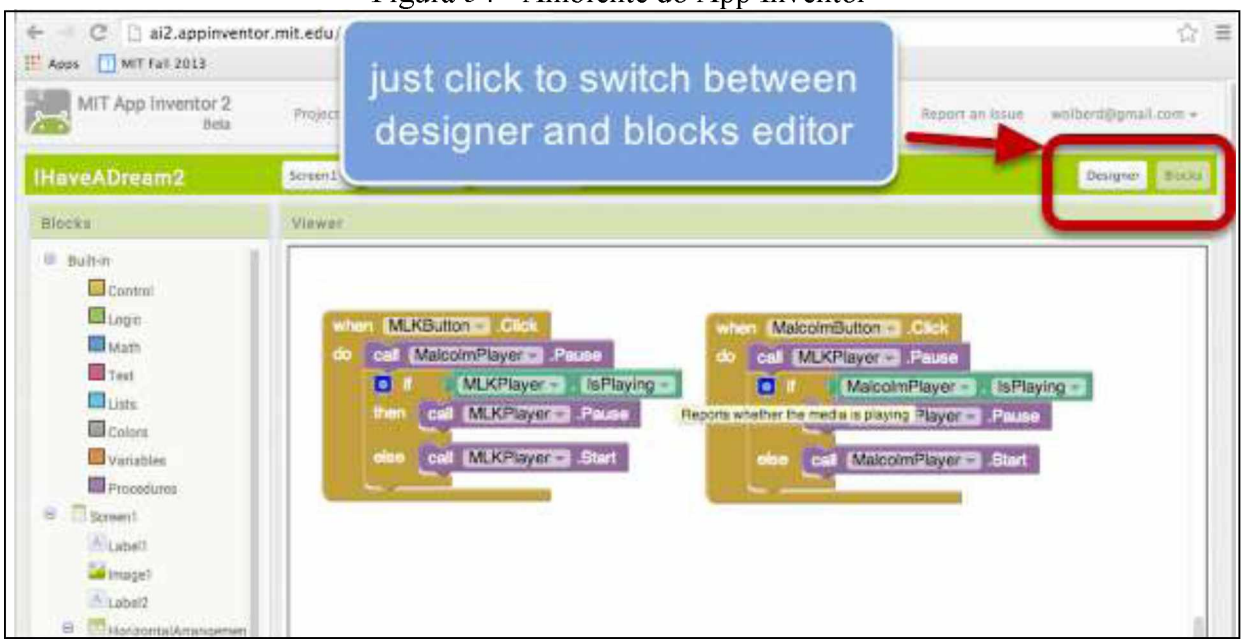
O aplicativo aparece no telefone passo a passo conforme o usuário adiciona as peças, podendo posteriormente testar o seu trabalho conforme o que ele construiu. Quando o trabalho estiver pronto, o usuário pode empacotar o seu aplicativo e produzir um aplicativo autônomo para instalá-lo.

Se o usuário não tiver um telefone Android, pode construir seus aplicativos usando o *emulador* Android, que é um software que pode ser executado em seu computador e que se comporta exatamente como o telefone.

O ambiente de desenvolvimento *App Inventor 2* tem suporte para Mac OS X, GNU / Linux e sistemas operacionais Windows, e para vários outros modelos de telefones Android populares. A aplicação que se pretende criar com *o App Inventor 2* poderá ser instalada em qualquer telefone Android, conforme os requisitos de sistema.

Antes de poder usar o *App Inventor* é preciso instalar o *Programa de Configuração App Inventor* do pacote no computador.

Figura 54 - Ambiente do App Inventor



Fonte: App Inventor (2015).

A parte de edição é executada no navegador, conforme se observa na Figura 54. Não é mais necessário o App Java para o Editor de Blocos. Basta clicar no botão Blocos no canto superior direito e editar os blocos para o aplicativo do usuário, diferentemente da versão 1.

Figura 55 - Interatividade do App Inventor

Fonte: App Inventor (2015).

É possível testar os aplicativos facilmente usando o Wi-Fi e o Companion MIT EA2, como demonstrado na Figura 55.

5.4 Desenvolvimento do projeto

A ideia de desenvolver este projeto para plataforma *mobile* é proporcionar uma maior e melhor flexibilização de utilização, uma vez que ele poderá ser instalado em praticamente qualquer celular com sistema operacional Android.

O aplicativo oferece um recurso portátil, de fácil acesso e manipulação, utilizado por grande parte da população atualmente (o telefone celular ou smartphone) que permite que o seu usuário esteja acessível em qualquer lugar, sobretudo se conectado à internet, de forma a poder usufruir melhor dos recursos oferecidos. Ele será disponibilizado ainda no *Google Play* para poder ser baixado/instalado de graça, sem custo algum para o usuário.

O propósito deste aplicativo é oferecer ao usuário orientação e também proporcionar maiores conhecimentos sobre segurança da informação no contexto das Smart TVs. Com tal objetivo, pretende-se que ele possua os seguintes recursos:

a) possibilidade de consultar as **Políticas de Privacidade** oficiais dos fabricantes de Smart TV;

b) uma **FAQ** com respostas esclarecedoras para as dúvidas do usuário no contexto da segurança das informações nas Smart TVs;
c) um **glossário** com os principais jargões, nomenclaturas e siglas existentes no universo da comunicação em Smart TV;
d) um **QUIZ** do conhecimento para educar o usuário-cliente em relação às nuances da segurança em Smart TV;
e) uma **pesquisa** para servir como fomentadora de informações técnicas, operacionais, culturais, de hábito e perfil do usuário utilizador de Smart TV, capaz de oferecer mais subsídios ao entendimento de suas necessidades e de servir para novas *features* do aplicativo, bem como para o fabricante.

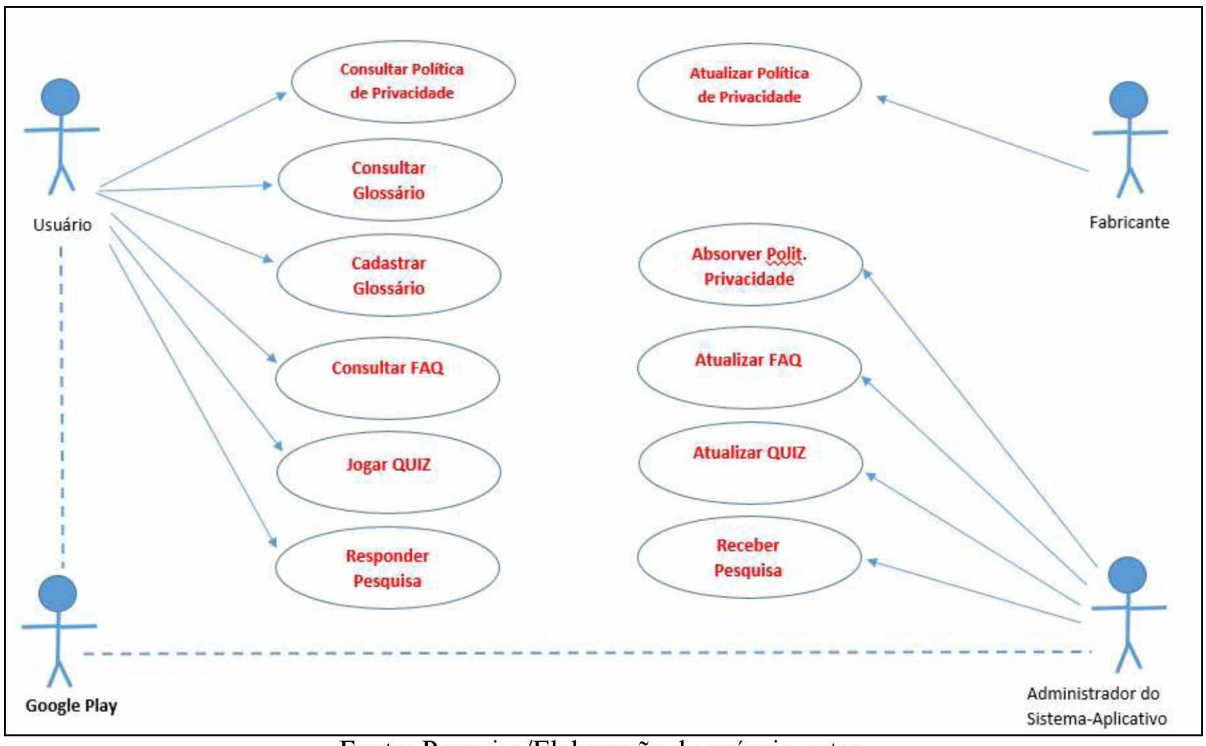
5.4.1 Use Case

Use Case (Figura 56) é uma sequência de ações que o sistema executa, produzindo um resultado de valor para o ator. Eis algumas de suas características:

a) modela o diálogo entre os atores e o sistema;
b) é iniciado por um ator para invocar uma certa funcionalidade do sistema;
c) é um fluxo de eventos completo e consistente.

O conjunto de todos os *Use Case* representa todas as situações possíveis de utilização do sistema.

Figura 56 - *Use Case*



Fonte: Pesquisa/Elaboração do próprio autor

5.5 Acessando o APP Inventor

5.5.1 Requisitos de sistema

Para usar o App Inventor, o computador do usuário deve atender aos seguintes requisitos de sistema:

a) Computador e sistema operacional:
   - Macintosh (com processador Intel): Mac OS X 10.5, 10.6+
   - Windows XP, Windows Vista, Windows 7 +
   - GNU / Linux: Ubuntu 8+, Debian 5+.

b) Navegador[29]
   - Mozilla Firefox 3.6 ou superior[30]
   - Apple Safari 5.0 ou superior
   - Google Chrome 4.0 ou superior

c) Telefone ou tablet (ou o emulador de tela)

[29] O Microsoft Internet Explorer não suporta o App Inventor. Os usuários do Windows devem usar o Chrome ou o Firefox.

[30] Se o Firefox for usado com a extensão No Script, será preciso rever a extensão

- Sistema operacional Android 2.3 ("Gingerbread") ou superior

Qualquer que seja o modelo, o telefone deve ter um cartão SD (físico ou virtual) instalado, ou então ele não funcionará com o *App Inventor*. A maioria dos telefones Android modernos tem cartões SD virtuais, de modo que esse é um problema apenas para os antigos celulares.

O *App Inventor* também funciona com muitos outros telefones Android, incluindo modelos da HTC, Samsung e Dell, mas, em muitos casos, é preciso baixar e instalar um software adicional do fabricante.

Uma outra opção seria o desenvolvimento com o Corona SDK, que é um kit de desenvolvimento de software (SDK) desenvolvido pela Corona Labs Inc. O Corona SDK permite que os programadores de software possam construir aplicações móveis para iOS, Android e Kindle, aplicativos de desktop para o Windows e OS X e aplicações de TV conectada para Apple TV e Android TV[31].

[31] Site oficial: https://coronalabs.com/.

6 EXEQUIBILIDADE E APLICABILIDADE

Vamos fazer aqui uma analogia com o mundo automobilístico, em que se tem vários modelos de carros com diferentes tecnologias, investimentos e performances. Para que isso seja possível, por "detrás das cortinas" são inúmeros os profissionais que trabalham operando, projetando, pensando e executando uma enorme quantidade de tarefas interligadas e conectadas, de forma que os processos vão se comunicando e convergindo para a fabricação e venda de um produto final que tem como objetivo conquistar a satisfação do cliente. Ou seja, um carro nasce após profunda pesquisa e estudo do mercado e de sua potencialidade de consumo, em que se deve de certa forma "modelar" em argila, aquilo que se conhece comercialmente como *CLAY*.[32]

Em suma, essa forma ou modelo, chamado de *Design Model,* é a primeira materialização de uma pesquisa de marketing, de maneira que o que é "modelado" naquele momento será possivelmente transformado em uma "máquina rodante", como no exemplo em questão.

O grande desafio a ser respondido, no caso do cenário que estamos exemplificando, é se será de fato possível fabricar o que se tem visivelmente elaborado em argila. Enfim, será possível fabricar aquilo que foi apresentado? Como diriam os americanos: "*Is it feasible*?". *Feasibility,* que em português significa *viabilidade*, é uma disciplina praticada nas montadoras que tem como finalidade analisar os riscos e a viabilidade de um sonho empresarial, de um projeto na fase de sua concepção.

Assim como se faz na indústria atualmente com a prática da gestão do conhecimento, por que também não utilizar o estudo de *feasibility* em ocasiões simples, como na restauração de uma casa, no planejamento de um casamento ou de uma viagem, no fechamento de um contrato de negócios, no desenvolvimento e na arquitetura de um software/aplicativo? Essa é uma forma de vislumbrar os riscos baseando-se na experiência passada.

Sendo assim, podemos afirmar que, para qualquer empreendimento, é muito válido analisarmos detalhe por detalhe a viabilidade, aplicabilidade e exequibilidade do projeto como parte da análise de riscos e, claro, levando em consideração a contribuição que ele trará não somente no âmbito econômico, mas, sobretudo, no âmbito cultural e social. De maneira que,

---

[32] Clay é o termo em inglês para argila plástica, basicamente um material de modelagem macio e maleável, composto de partículas de PVC (*Polyvinyl Chloride*) que, quando aquecidas em baixa temperatura e por um determinado tempo, se fundem e resultam em um plástico duro, resistente e durável.

ao se utilizar essa prática, certamente aumenta-se o grau de confiabilidade do produto que se planeja oferecer.

6.1 Orçamento

No caso de um projeto destinado à aplicação prática, como um produto ou plano de aplicação, o campo que demarca todo e qualquer tipo de recurso utilizado é absolutamente necessário.

Na divisão tradicional, os recursos são divididos em três tipos: material humano (Quadro 11), de consumo (Quadro 12) e de custeio (Quadro 13) (UFU, 2014).

Quadro 11 - Recursos: material humano

MATERIAL HUMANO				
Qtd.	**Recurso**	**Valor hora/recurso**	**Valor Unitário (mês)**	**TOTAL**
1	Programador Android Mobile	R$ 10,45	R$ 2.506,81	R$ 2.506,81
1	Administrador de Banco de Dados (DBA) Junior.	R$ 10,39	R$ 2.494,24	R$ 2.494,24
1	Analista de Suporte Técnico em Informática – Help Desk Júnior	R$ 5,75	R$ 1.382,03	R$ 1.382,03
1	Arquiteto da Informação / UX Design – Pleno.	R$ 18,94	R$ 4.546,72	R$ 4.546,72
1	Analista de Negócios Web Sênior	R$ 20,67	R$ 4.961,69	R$ 4.961,69
1	Administrador de Redes Pleno	R$ 12,37	R$ 2.969,19	R$ 2.969,19
1	Analista de Requisitos Sênior	R$ 24,80	R$ 5.954,35	R$ 5.954,35
1	Analista de Testes Sênior	R$ 15,28	R$ 3.669,42	R$ 3.669,42
1	Analista de Negócio/Processo	R$ 20,83	R$ 5.000,00	R$ 5.000,00
1	Analista de Segurança da Informação Pleno	R$ 15,43	R$ 3.705,12	R$ 3.705,12
TOTAL				**R$ 37.189,57**

Fonte: Pesquisa/Elaboração do próprio autor.

Quadro 12 - Recursos: material de consumo

MATERIAL de CONSUMO			
Qtd.	**Recurso**	**Valor unitário**	**TOTAL**
1	Quadro para planejamento mensal em alumínio standart 60x90 cm – Cortiarte	R$ 103,92	R$ 103,92
1	Quadro branco standard 120 x 150 cm – Cortiarte	R$ 138,90	R$ 138,90
2	Pincéis	R$ 10,00	R$ 10,00
1	Bloco adesivo Post-It Cubo Neon com 4 cores, 4,76 cm X 4,76 cm e 400 folhas	R$ 24,90	R$ 24,90
1	Flip Chart standard em madeira MDF branco Cortiarte	R$ 95,90	R$ 95,90
1	Kit canetas BIC	R$ 8,00	R$ 8,00
1	Pacote telefone fixo + internet 10 mb	R$ 80,00 (mês)	R$ 80,00
1	Pacote de dados e telefone celular	R$ 40,00 (mês)	R$ 40,00
1	CD/DVD	R$ 20,00	R$ 20,00
1	Apagador	R$ 5,00	R$ 5,00
TOTAL			**R$ 526,62**

Fonte: Pesquisa/Elaboração do próprio autor.

Quadro 13 - Recursos: material de custeio

MATERIAL de CUSTEIO			
Qtd.	**Recurso**	**Valor Unitário**	**TOTAL**
1	Notebook Lenovo Proc.Intel i7, 8G , 1Tb	R$ 2.800,00	R$ 2.800,00
2	Sistema Operacional Microsoft Windows 8.1 Pro - 32 / 64 Bits - Versão Full - FQC-07325	RS 341,05	RS 682,10
1	Pen-drive 8GB - Sandisk - Cruzer Blade	R$ 14,90	R$ 14,90
1	Smartphone, Android, 8G	R$ 1.631,00	R$ 1.631,00
1	HD Externo Toshiba Canvio Connect 5400 rpm 500GB USB 3.0 Black	R$ 210,59	R$ 210,59
1	Modem D-Link ADSL2+ DSL-2500E/ZBRII	R$ 68,77	R$ 68,77
1	Roteador Linksys Wrt54gl 802.11b/g 54mbps 2.4ghz	R$ 549,90	R$ 549,90
1	Monitor Philips V-line 193V5LSB2 LCD 18.5 Polegadas	R$ 356,67	R$ 356,67
2	Mouse Microsoft 1850 Wireless	R$ 58,41	R$ 116,82
1	Teclado Wireless	R$ 74,61	R$ 74,61
1	Licença (3 máquinas) antivírus BIT-DEFENDER 2016	R$ 103,00	R$ 103,00
TOTAL			**R$ 5926,26**

Fonte: Pesquisa/Elaboração do próprio autor.

7 CONSIDERAÇÕES FINAIS

Após a realização de nosso estudo, concluímos que a arquitetura do novo aparelho televisivo está dividida em camadas, formando um modelo de estrutura convergente e de novos serviços oferecidos pela Smart TV que hoje suporta e está preparada para novas integrações e interações.

Foi possível notar também que *hackear* uma Smart TV provavelmente não trará o mesmo retorno financeiro que *hackear* um computador ou smartphone, pelo fato de que as informações mais importantes e confidenciais do usuário ainda estão armazenadas e transitam mais comumente por meio dos dois últimos tipos de equipamento, e não de uma Smart TV.

No entanto, ressalta-se que a privacidade é muito importante, de maneira que, como vimos, é justamente a política de privacidade que irá tentar ajudar a definir e deixar claro quais tipos de informações cadastrais absorvidas em tempo real pela Smart TV serão de fato manipuladas pelo fabricante quando o usuário estiver on-line. Esse é um dos lados da moeda. O outro, como também vimos, se refere justamente às vulnerabilidades e brechas trazidas de fábrica (por falta de maiores cuidados da engenharia de hardware e software do fabricante), que permitirão supostos ataques de pessoas mal-intencionadas externamente.

Outro fator importante é que a Smart TV é um ambiente perfeito para vigilância, pois, conforme retratamos, algumas delas possuem recursos de captura de som e imagem com câmera embutida. É importante lembrar que as Smart TVs estão cada vez mais inseridas em locais públicos e privados, e que mesmo desligadas podem receber sinais (caso tenham sido desligadas apenas via controle remoto). Sendo assim, é preciso que o usuário esteja atento, como descrito no decorrer deste trabalho, para o fato não somente de estar on-line, na internet principalmente, bem como para o perigo de não blindar a rede interna (roteador – Wi-Fi) onde sua Smart TV está inserida. Ele deve se preocupar ainda com questões relativas a outros sistemas físicos cibernéticos existentes no contexto da Internet das Coisas.

Quanto ao contexto do Sistema Operacional, do *middleware* e dos aplicativos, todos estes contidos na arquitetura da Smart TV, deve-se repensá-los como plataformas robustas, compatíveis e bem testadas (como, por exemplo, o Android), que colaborariam no âmbito da exploração do desenvolvimento e implementação de aplicativos mais flexíveis.

Há também uma padronização dessa arquitetura pelo menos em relação ao kernel (núcleo principal, que seria o Sistema Operacional + *Middleware*, deixando as aplicações à vontade para cada fabricante), que permitiria uma espécie de força-tarefa unificada e

homogênea se todos os fabricantes de Smart TV desenvolvessem essa arquitetura com um padrão central e menos personalizações. Ela poderia resolver de forma mais eficiente futuras vulnerabilidades que viessem a surgir.

No relatório lançado pelo Gartner que, chamado "*Prevenção é inútil em 2020: proteja a informação através do monitoramento persuasivo e de Inteligência Coletiva*", destacam-se dois grandes desafios. A segurança da informação, que não pode mais evitar ataques "direcionados e avançados", e "grandes gastos com segurança da informação têm como foco a prevenção de ataques e não tem sido feito o suficiente para o monitoramento de capacidades de respostas de segurança" (GARTNER, 2014).

Essas são recomendações que merecem destaque, de maneira que seria importante que os fabricantes de Smart TV investissem em sua capacidade de resposta a incidentes, definindo uma equipe capaz de mapear processos para entender rapidamente o alcance e o impacto de uma violação detectada em seus aparelhos.

O fato é que ignorar o fenômeno da TV digital no país e no mundo, com a inserção e evolução cada vez mais forte da Smart TV como meio de comunicação, entretenimento, informação e interação, é desconsiderar as estatísticas e pesquisas que demonstram a sua importância.

> A TV continua a ser a principal fonte de informação no País, com 55,9% da preferência, seguida pela internet (20,4%), pelo jornal impresso (10,5%), pelo rádio (7,8%), pelas redes sociais (2,7%), pela versão on-line dos jornais impressos (1,8%), pela revista impressa (0,8%) e pela versão on-line das revistas (0,1%). Com relação às fontes de informações mais acessadas no dia a dia do brasileiro, a televisão é vista por praticamente todos os entrevistados, somando 99,3%, seguida por rádio (83,5%), jornal impresso (69,4%), internet – sites de notícias e blogs de jornalistas (52,8%), revista impressa (51,1%), redes sociais – Twitter, Orkut, Facebook, etc. (42,7%), pela versão on-line dos jornais impressos (37,4%) e pela versão on-line das revistas impressas (22,8%). (ABERT,2016. p.65).

Partindo-se da premissa de que a televisão é o meio de comunicação de massa mais forte, que a tendência de todos os televisores é ser tornarem uma Smart TV, e que por meio dela o usuário consegue acessar a internet, ler jornal, ouvir rádio, entrar em redes sociais, blogs, ler revistas e e-books, chegamos à conclusão, não por mera dedução, mas pelo raciocínio lógico, que a disseminação viral, absoluta e inevitável da Smart TV em todas as classes sociais fará com que ela seja de fato um dos tipos de aparelho/recurso (mesmo que não tenha mobilidade) mais presentes nos diferentes lares e estabelecimentos da sociedade moderna. Sendo assim, fica consideravelmente comprovada a necessidade legítima, cultural e socialmente justificável de políticas públicas que tratem com a devida atenção esse fenômeno da comunicação educativa e cada vez mais tecnológica, para que se possa ter, entender,

usufruir e explorar a chamada Smart TV de diferentes formas e em diversas e situações, sem que para isso o seu usuário tenha que temer pela segurança de seus dados pessoais.

REFERÊNCIAS

4LINUX. *O que é Middleware*. Disponível em: <https://www.4linux.com.br/o-que-e-middleware>. Acesso em: 2 abr. 2016.

ABERT. *Estatísticas de comportamento*. Disponível em: <http://www.abert.org.br/web/index.php/dados-do-setor/estatisticas/estatisticas-de-comportamento>. Acesso em: 3 abr. 2016.

ABREU, D. Melhores práticas para classificar as informações. *Módulo e-Security Magazine*, São Paulo, ago. 2001. Disponível em: <http://www.modulo.com.br>. Acesso em: 31 out. 2015.

ALBERTA. Governament of Alberta. *Information Security Classification*. Alberta, Feb. 2005. Disponível em: <http://www.im.gov.ab.ca/publications/pdf/InfoSecurityClassification.pdf>. Acesso em: 31 out. 2015.

APP INVENTOR.ORG.*App Inventor 2 Changes*. Disponível em: <http://www.appinventor.org/appInventor2Changes>. Acessado em: 7 nov. 2015.

APPOLINÁRIO, F. *Dicionário de metodologia científica*: um guia para a produção do conhecimento científico. São Paulo: Atlas, 2009.

ATMEL. *Introdução*: IEEE 802.15.4. Disponível em: <http://www.atmel.com/pt/br/products/Wireless/802154/start_now.aspx>. Acesso em: 10 abr. 2016.

ARENDT, H. *A condição humana*. 10. ed. Trad. Roberto Raposo. Rio de Janeiro: Forense Universitária, 2009.

ARISTÓTELES. *Política*. Rio de Janeiro: Ediouro, 1988.

ARRUDA CONSULT. *Matriz de priorização CEB*: aprenda usar e baixe modelo grátis. 17 fev. 2015. Disponível em; http://www.arrudaconsult.com.br/2015/02/matriz-de-priorizacao-ceb-aprenda-usar.html . Acesso em: 4 dez. 2015. ARRUDA

ASCENSÃO, J. de O. Sociedade da Informação e mundo globalizado. *Boletim da Faculdade de Direito da Universidade de Coimbra*, Coimbra, 2003.

BADABRASIL. SDK. 2011. Disponível em: <http://www.badabrasil.com.br/2011/07/o-que-e-sdk.html Acesso em: 17 nov. 2015.

BARROS, A .J. S.; LEHFELD, N. A. S. *Fundamentos de metodologia*: um guia para iniciação cientifica. 2 Ed. São Paulo: Makron Books, 2007.

BENOIT, H. *Digital television*. Satellite, cable, terrestrial, IPTV, mobile TV in DVB. 4. ed. Paris: Focal Press, 2008.

BLOGGER. Disponível em: <http://4.bp.blogspot.com/n45rq5PpO7c/USfnRxG5zJI/AAAAAAAAFhY/NyQqJNcF98/s1600/V+Familia_tv_antiga.jpg>. Acesso em: 17 nov. 2015.

BRAGA, A. M.; RESTANI, G. S. Introdução à segurança de aplicações para a TV digital interativa brasileira. In: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, 10., 2010, Fortaleza. Cap. 5. Disponível em: <http://ceseg.inf.ufpr.br/anais/2010/04_minicursos/minicurso_05.pdf>. Acesso em: 2 jan. 2016.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. [Lei do Marco Civil da Internet]. *Diário Oficial da União*, Brasília, DF, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 28 dez. 2015.

BRASIL. Ministério da Ciência e Tecnologia. *Livro Branco*: Ciência, Tecnologia e Inovação. Brasília, DF, jun. 2002. Disponível em: <http://www.cgee.org.br/arquivos/livro_branco_cti.pdf>. Acesso em: 22 dez. 2015.

BRASIL. Ministério da Educação. *Base Nacional Comum Curricular*. Brasília, DF, 2015. Disponível em: <http://basenacionalcomum.mec.gov.br/#/site/base/o-que>. Acesso em: 21 out. 2015.

BRASILEIROS aderem aos recursos da TV conectada. *Valor Econômico*,São Paulo, 20 nov. 2015. Disponível em: <http://www.valor.com.br/empresas/4334868/brasileiros-aderem-aos-recursos-da-tv-conectada?utm_source=newsletter_tectel&utm_medium=02122015&utm_term=brasileiros+aderem+aos+recursos+da+tv+conectada&utm_campaign=informativo&NewsNid=4310116 . Acesso em: 28 nov. 2015.

BRIGATTO, Gustavo. Brasileiros aderem aos recursos da TV conectada. *Valor Econômico-Empresas*, São Paulo, 30 nov. 2015. Notícias. Publicado pela AESP. Disponível em: <http://www.aesp.org.br/noticias_view_det.php?idNoticia=13488>. Acesso em: 22 nov. 2016.

BASTOS, C. R. *Curso de direito constitucional*. 21. ed. São Paulo: Saraiva, 2000.

BROWN, J. D. *Library classification and cataloguing*. [S.l: s.n.], 1916.

CAMPVIDEO. Ilha de edição video profissonal. Disponível em: <http://www.campvideo.com.br/#!product/prd1/1371761341/ilha-de-edi%C3%A7%C3%A3o-v%C3%ADdeo-profissional> Acesso em: 8 ago. 2016.

CAPURRO, R. Epistemologia e ciência da Informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 5., 2003, Belo Horizonte. *Anais*... Belo Horizonte: Escola Ciência da Informação, Universidade Federal de Minas Gerais, 2003.

CAPURRO, Rafael. Privacy: an intercultural perspective. Ethics and Information Technology, [s.l.], v. 7, p. 37-47, 2005.

CARTOONSTOCK. If this is a smart TV, then why does it show reality shows? Disponível em: <https://www.cartoonstock.com/cartoonview.asp?catref=jknn956>. Acesso em: 22 maio. 2016.

CELLARD, A. A análise documental. In: POUPART, J. et al. *A pesquisa qualitativa*: enfoques epistemológicos e metodológicos. Petrópolis: Vozes, 2008.

CHIZZOTTI, A. *A pesquisa em ciências humanas e sociais*. São Paulo: Cortez, 2005.

COLENGHI, V. M. *O&M e qualidade total*: uma integração. Rio de Janeiro: Qualitymark, 1997.

COMPRARTV, Quem inventou a televisão? – Guias . Disponível em: <http://comprartv.com.br/quem-inventou-televisao/> . Acesso em: 10 junho. 2016.

CONSUMENTENBOND.*Mais privacidade com TV inteligentes*: dicas. Disponível em: <http://www.consumentenbond.nl/internet-privacy/extra/smart-TV-privacytips/>. Acesso em: 29 dez. 2015.

CVMULTIMÉDIA. O que é Set-Top Box? Disponível em: <http://www.cvmultimedia.cv/o-que-%C3%A9-set-top-box>. Acesso em: 20 dez. 2015.

DAGNINO, R. *Tecnologia social*: uma estratégia para o desenvolvimento. Rio de Janeiro: Fundação Banco do Brasil, 2004.

DAGNINO, R.; GOMES, E. Sistema de inovação social para prefeituras. In: CONFERÊNCIA NACIONAL DE CIÊNCIA E TECNOLOGIA PARA INOVAÇÃO, 2000. *Anais*... São Paulo: [s.n.], 2000.

DAVENPORT, T. H. *Ecologia da informação*: porque só a tecnologia não basta para o sucesso da era da informação. Trad. Bernadete Siqueira. São Paulo: [s.n.], 1998.

DIERKS, T.; ALLEN, C. *The TLS Protocol*: Version 1.0. [S.l.]: The Internet Society, Jan. 1999. IETF RFC 2246. Disponível em: <http://www.ietf.org/rfc/rfc2246.txt>. Acesso em: 31 maio 2015.

DIGITAL LIVING NETWORK ALLIANCE. *Consumer Home*. Disponível em: <www.dlna.org>. Acesso em: 31 out. 2015.

ELECTRONIC FRONTIER FOUNDATION. *DMA*. Disponível em: <https://www.eff.org/>. Acesso em: 18 abr. 2016a.

ELECTRONIC FRONTIER FOUNDATION. Disponível em: <https://www.eff.org/>. Acesso em: 18 abr. 2016b.

ELETRONICDESIGN. *What's The Difference Between ZigBee And Z-Wave?* 2015. Disponível em: <http://electronicdesign.com/communications/what-s-difference-between-zigbee-and-z-wave>. Acesso em: 22 maio 2016.

ELO, Meios de Comunicação, ELMC2015ANADUARTE. Disponível em: <http://www.elo.pro.br/cloud/aluno/atividade.php?id=1168&etapa=8> Acesso em: 10 julho 2016.

ESPINHARA, J.; ALBUQUERQUE, U. *SmartTVecurity*: for fun and non-profit. Disponível em: <http://pt.slideshare.net/urma_/smarttv-hacking>. Acesso em: 18 abr. 2016.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. *Digital Vídeo Broadcasting (DVB)*. Multimedia Home Platform (MHP) Specification 1.1.1. v. 1.1.2. Rev.1. França: 2003.

FABRICANTES de TV investem em telas imensas, imagem e conectividade. *Diário Gaucho*, Porto Alegre, 1 ago. 2016. Noticias. A TV contra-ataca. Disponível em: <http://diariogaucho.clicrbs.com.br/rs/dia-a-dia/noticia/2016/08/fabricantes-de-tv-investem-em-telas-imensas-imagem-e-conectividade-7047514.html>. Acesso em: 11 ago. 2016.

FERREIRA, G. M. *Curso de direito constitucional*. São Paulo: Saraiva, 2014.

FIGUEIREDO, N. M. A. *Método e metodologia na pesquisa científica*. 2. ed. São Caetano do Sul: Yendis, 2007.

FORTUNATO, I. Civilização em crise: grotesco e histeria devoram o jornalismo. *Revista E-COM*, Belo Horizonte, v. 5, n. 1, p. 124-138, 2010.

GALPERIN, H. Comunicación e integraciónenla era digital: um balance de la transición hacia la televisión digital en Brasil y Argentina. *Revista Eletrônica Telos*, Madrid, 2003.

GARTNER. *Gartner Says 85 Percent of All Flat-Panel TVs Will Be Internet-Connected Smart TVs by 2016, STAMFORD, Conn., December 18, 2012*. Disponível em: <http://www.gartner.com/newsroom/id/2280617>. Acesso em: 13 Agosto. 2016.

GARTNER. *Gartner's hype cycle special report for 2011*. [S.l.], 2012. Disponível em: <http://www.gartner.com/technology/research/hype-cycles/>. Acesso em: 31 out. 2015.

GARTNER. *Prevention is Futile in2020*: Protect Information Via Pervasive Monitoring and Collective Intelligence. From the Gartner Files. 2014. Disponível em: <http://imagesrv.gartner.com/media-products/pdf/ObserveIT/ObserveIT_issue1.pdf>. Acesso em: 18 abr. 2016.

GEORGIA. Supreme Court of Georgia. *Pavesich v. New England Life Insurance CO. et al.* 14 May 1904. Disponível em: <http://faculty.uml.edu/sgallagher/pavesich_v.htm>. Acesso em: 5 jun. 2015.

GIL, A. C. *Como elaborar projetos de pesquisa*. 4. ed. São Paulo: Atlas, 2002.

GOLDENBERG, M. *A arte de pesquisar*: como fazer pesquisa qualitativa em ciências sociais. 2002. Disponível em: <http://www.ufjf.br/labesc/files/2012/03/A-Arte-de-Pesquisar-Mirian-Goldenberg.pdf>. Acesso em: 23 nov. 2015.

GOMES, H. S.; CAOLI, C. Mais de 50% de domicílios brasileiros têm apenas TV de tubo, diz IBGE. *G1*, 29 abr. 2015. Disponível em:

<http://g1.globo.com/tecnologia/noticia/2015/04/mais-de-50-de-domicilios-brasileiros-tem-apenas-tv-de-tubo-diz-ibge.html>. Acesso em: 23 nov. 2015.

HARDESTY, L. As raízes do MIT do novo software do Google. *MIT Notícias Office*, [s.l.], 19 ago. 2010.

HONNETH, A. A textura da justiça: sobre os limites do procedimentalismo contemporâneo. *Civitas*, Porto Alegre, v. 9, n. 3, p. 345-368, set./dez. 2009.

HONNETH, A. *Luta por reconhecimento*: a gramática moral dos conflitos sociais. São Paulo: Ed. 34, 2003.

INSTITUTO EUVALDO LODI. Núcleo Central. *TV digital*: qualidade e interatividade. Brasília, DF: IEL/NC, 2007.

INTERNATIONAL DATA CORPORATION. *Smartphone OS Market Share, 2015 Q2*. Califórnia, 2015. Disponível em: <http://www.idc.com/prodserv/smartphone-os-market-share.jsp>. Acesso em: 31 out. 2015.

JOHN LOGIE BAIRD. In: BIOGRAPHY.COM. Disponível em: <http://www.biography.com/people/john-logie-baird-9195738>. Acesso em: 4 nov. 2015.

JOHN LOGIE BAIRD (1888 - 1946). *BBC*, London, 2014. History. Disponível em: <http://www.bbc.co.uk/history/historic_figures/baird_logie.shtml>. Acesso em: 22 nov. 2016
JOHNSON, S. *Cultura dainterface*: como o computador transforma nossa maneira de criar e comunicar. Rio de Janeiro: J. Zahar, 2001.

JWSAT. [*História*: TV]. Disponível em: <http://www.jwsat.com.br/noticias/historia_tv.pdf>. Acesso em: 21 nov. 2015.

KEPNER, C.; TREGOE, B. *O novo administrador racional*. São Paulo: Makron Books, 1991.

KOREA UNIVERSITY. Center for Information Security Technologies. Hacking, Surveilling, and Deceiving Victims on SmartTV. 2013. Disponível em: <https://media.blackhat.com/us-13/US-13-Lee-Hacking-Surveilling-and-Deceiving-Victims-on-Smart-TV-Slides.pdf>. Acesso em: 7 jan. 2016.

KUHLEN, R. I*nformationsethik*: Umgang mit Wissen und Information in elektronischen Räumen. Konstanz: Universitätsverlag Konstanz, 2004.

LAFER, C. *A reconstrução dos direitos humanos*. São Paulo: Companhia das Letras, 1998.

LAVILLE, C.; DIONNE, J. *A construção do saber*. Adaptação da obra de Lana Mara Siman. São Paulo: Artmed, 2008. Disponível em: <http://disciplinas.stoa.usp.br/pluginfile.php/311372/mod_resource/content/1/Laville%2C%20Christian%20%20Dionne%2C%20Jean_A%20Construcao%20do%20Saber%20%28completo%29.pdf>. Acesso em: 22 maio 2016.

LCD-TV – By Guide. Top 10 TVs Best Sellers. - INCLUDES LED, 4K, AND OLED TVS by Robert Wiley. Disponível em: https://lcdtvbuyingguide.com/top10.shtml . Aceso em: 11 já. 2017.

LEMOS, A. L. M. *Anjos interativos e retribalização do mundo*: sobre interatividade e interfaces digitais. [S.l.: s.n], 1997.

MARCONI, M. A.; LAKATOS, E. M. *Fundamentos de metodologia científica*. São Paulo: Atlas, 2007.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY.What is App Inventor? Disponível em: <http://appinventor.mit.edu/explore/content/what-app-inventor.html>. Acesso em: 22 nov. 2015a.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY.*Setting Up App Inventor 2*. Disponível em: <http://appinventor.mit.edu/explore/content/what-app-inventor.html>. Acesso em: 22 nov. 2015b.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY.*Installing and Running the Emulator in AI2*. Disponível em: <http://appinventor.mit.edu/explore/ai2/setup-emulator.html>. Acesso em: 22 nov. 2015c.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY.*Installing App Inventor 2 Setup on Windows*. Disponível em:<http://appinventor.mit.edu/explore/ai2/windows.html>. Acesso em: 22 nov. 2015d.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY.*Setting up App Inventor*. Disponível em: <http://appinventor.mit.edu/explore/ai2/setup>. Acesso em: 22 nov. 2015e.

McLUHAN, M. *Os meios de comunicação como extensões do homem*. São Paulo: Cultrix, 1995.

MIT AI2 COMPANION. Disponível em: <https://play.google.com/store/apps/details?id=edu.mit.appinventor.aicompanion3&hl=pt_BR>. Acesso em: 4 nov. 2015.

MONTEZ, C.; BECKER, V. *TV digital interativa*: conceitos, desafios e perspectivas para o Brasil. 2. ed. Florianópolis: Ed. da UFSC, 2005.

MORAN, J. M. *A interatividade na televisão e nas redes eletrônicas*. São Paulo: EDUSP, 2002.

MORIN, E. *O enigma do homem*. Para uma nova antropologia. Rio de Janeiro: Zahar, 1975.

MORIN, E. *O enigma do homem*. Rio de Janeiro: Zahar, 1979.

MORIN, E. *Introdução ao pensamento complexo*. Lisboa: Instituto Piaget, 1991.

NAVARROS, A. M. N. de P.; LEONARDOS, G. *Informational privacy*: origin and foundations in American Law. 2011. Disponível em:

<http://www.publicadireito.com.br/artigos/?cod=34f9a343f945196b>. Acesso em: 31 out. 2015.

NFC, About Near Field Communication. Disponivel em: <http://nearfieldcommunication.org/about-nfc.html>. Acesso em: 12 nov. 2016.

NOBLETT, T. *Business of IT*: Understanding Regulatory Compliance. 2006. Disponível em: <https://technet.microsoft.com/en-us/magazine/2006.09.businessofit.aspx>. Acesso em: 17 dez. 2015.

NOVAES, H. T.; DAGNINO, R. O fetiche da tecnologia. *Revista Organizações & Democracia*, Marília, n. 2, v. 5, 2004.

NPD GROUP. *TVcreen Application Usage*. Disponível em: <https://www.npdgroupblog.com/wp-content/uploads/2012/12/CI-Connect-Home-Blog.jpg>. Acesso em: 8 nov. 2015.

OLIVEIRA, D. de P. R. de. *Planejamento estratégico*: conceitos, metodologias e práticas. São Paulo: Atlas, 1992

OLIVEIRA, J. L. de. *Texto acadêmico*. Petrópolis: Vozes, 2005.

OLIVEIRA, Z. M. R. de (Org.). *Educação infantil*: muitos olhares. 3. ed. rev. São Paulo: Cortez, 1996.

OLIVEIRA, Z. M. R. de. *Educação infantil*: fundamentos e métodos. São Paulo: Cortez, 2002. (Docência em formação).

PAES, A.; ANTONIAZZI, R. *Padrões de Middleware para TV Digital*. Niterói: Universidade Federal Fluminense, Centro Tecnológico, Departamento de Engenharia de Telecomunicações, 2005. Disponível em: <http://www2.midiacom.uff.br/downloads/pdf/paes_2005a.pdf>. Acesso em: 10 jun. 2005.

PEIXOTO, M. C. P. *Business Model Canvas*: C.O.S.I. 2015. Disponível em: http://canvas.sebraecanvas.com/6399c6f8c0af4c09a15827fdd7412cab/18848/. Acesso em: 17 jan. 2016.

PELTIER, T. R. *Standardinzing Information Classification*. Disponível em: <http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci995767,00.html?Offer=SEcpcc42005>. Acesso em: 31 out. 2015.

PEROVANO, D. G. *Manual de metodologia científica*: para segurança pública e defesa social. 1. ed. São Paulo: Juruá, 2014.

PINTO, Á. V. *O conceito de tecnologia*. Rio de Janeiro: Contraponto, 2005. 2 v.

PIPELINE PUBLISHING. *Hacking 4.0*: What will they hack next? Disponível em: <http://www.pipelinepub.com/security/hacking_threats/3>. Acesso em: 20 abr. 2016.

POKÉMON GO gera dúvidas sobre a privacidade dos jogadores. *Folha de S. Paulo*,

São Paulo, 13 jul. 2016. Mercado. Disponível em: <http://www1.folha.uol.com.br/mercado/2016/07/1791219-pokemon-go-gera-duvidas-sobre-a-privacidade-dos-jogadores.shtml> . Acesso em: 10 jun. 2016.

PORTAL EDUCAÇÃO. *Arquiteura da TV digital*. 24 abr. 2013. Disponível em: <http://www.portaleducacao.com.br/iniciacao-profissional/artigos/45876/arquitetura-da-tv-digital#>. Acesso em: 17 dez. 2015.

PORTO, E.; CIRNE, L. Mapeamento sobre a Interatividade na TV Digital. Interactivity survey in the digital television. *Revist de Estudos da Comunicação*, Curitiba, v. 10, n. 22, p. 169-178, maio/ago. 2009. Disponivel em: <http://www2.pucpr.br/reol/index.php/comunicacao?dd99=pdf&dd1=3585>. Acesso em: 13. fev. 2016.

PORTAL ABANT, Noticias – Resoluçao 510 – [2016]. Disponível em: <http://www.portal.abant.org.br/images/Noticias/Resolu%C3%A7%C3%A3o_510__16_DO.pdf>. Acesso em: 02 nov. 2016.

RAMOS, A. *Classificação da informação*: teoria e prática. [S.l.], ISSA, [2002]. Disponível em: <http://static1.1.sqspcdn.com/static/f/454486/8555837/1284551483920/Classificao+da+Informao+-+Teoria+e+prtica.pdf?token=E%2BteQb4oE0CjTDk8bNfT46csPAg%3D>. Acesso em: 31 out. 2015.

RAPID TV. *Quase metade dos dispositivos de entretenimento domésticos estão conectados*. 3 maio 2013. Disponível em: <http://convergecom.com.br/teletime/03/05/2013/quase-metade-dos-dispositivos-de-entretenimento-domesticos-estao-conectados/>. Acesso em: 7 nov. 2015.

REVULN. SmartTV: IN~~Seeurity~~. Disponível em: <http://revuln.com/files/Ferrante_Auriemma_SmartTV_Insecurity.pdf>. Acesso em: 17 abr. 2016.

RIBEIRO, G. Devo proteger minha Smart-TV contra vírus e ataque hackers? *TechTudo*, Vida Digital, 30 jun. 2014. Disponível em: <http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2014/06/devo-proteger-minha-smart-tv-contra-virus-e-ataques-hackers-veja-como.html>. Acesso em: 22 mar. 2016.

RODOTÀ, S. *A vida na sociedade da vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SCHERMER, W.; FALOT, N. *Analyse privacyvoorwaarden Smart-TV in opdracht van de Consumentenbond*. Aug. 2014. Disponível em: <http://www.consumentenbond.nl/campagne-content/privacy/media/201400820Onderzoek_privacyvoorwaarden_smarttv.pdf>. Acesso em: 1 dez. 2015.

SEBRAE. Quadro de modelo de negócios: para criar, recriar e inovar. Disponível em: <http://www.sebrae.com.br/sites/PortalSebrae/bis/Quadro-de-modelo-de-neg%C3%B3cios:-para-criar,-recriar-e-inovar>. Acesso em: 14 dez. 2015.

SÊMOLA, M. *Gestão da segurança da informação*: uma visão executiva. Rio de Janeiro: Campus, 2003.

SIRIHAL, A. B.; LOURENÇO, C. de A. Informação e conhecimento: aspectos filosóficos e informacionais. *Informação &Sociedade*: estudos, João Pessoa, v. 12, n. 1, p. 67-92, 2002. Disponível em <http://www.ies.ufpb.br/ojs2/index.php/ies/article/viewFile/154/148>. Acesso em: 9 out. 2015.

O SISTEMA operacional GNU. Disponível em: <http://www.gnu.org/philosophy/free-sw.html>. Acesso em: 9 out. 2015.

SOARES, D. Como controlar sua Smart -TV pelo Android? 2015. Disponível em: <http://www.escolaandroid.com/como-controlar-smart-tv-pelo-android/>. Acesso em: 17 fev. 2016.

SOFTWARE FREEDOM CONSERVANCY. Disponível em: <https://sfconservancy.org/>. Acesso em: 31 out. 2015.

STACK OVERFLOW. *SmartTV development for starters*. Disponível em: <http://stackoverflow.com/questions/12940572/smarttv-development-for-starters>. Acesso em: 22 maio 2016.

TECNOTV.COM.BR. *5 dúvidas mais comuns sobre a TV com acesso a internet* – Smart TV. Disponível em: <http://tvcominternet.com.br/duvidas-comuns-tv-com-acesso-a-internet/>. Acesso em: 22 nov. 2016.

TELEVISÃO. In: WIKIPEDIA. Disponível em: <https://pt.wikipedia.org/wiki/Televis%C3%A3o>. Acesso em: 5 nov. 2015.

UNIVERSIDADE FEDERAL DE UBERLÂNDIA. Programa de Pós-Graduação em Tecnologias, Comunicação e Educação. *Diretrizes para elaboração do relatório de qualificação e relatório final (dissertação, plano de aplicação ou produto)*. Uberlândia, 2014. Disponível em: <http://www.ppgce.faced.ufu.br/sites/ppgce.faced.ufu.br/files/Anexos/Bookpage/DIRETRIZES_QUALIFICACAO_DEFESA_PPGCE_0.pdf>. Acesso em: 16 dez. 2015.

WARREN, S.; BRANDEIS, L. The Right to Privacy. *Harvard Law Review*, Cambridge, v. 4, n. 5, p. 193-220, 1890. Disponível em: <http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf>. Acesso em: 25 de maio 2012.

WEBER, T. *Ética e filosofia política*: Hegel e o formalismo Kantiano. Porto Alegre: EDIPUCRS, 1999.

WEMISSOURTV.COM. *The Evolution of TV*. Disponível em: <http://www.wemissourtv.com/wmotv/wp-content/uploads/2015/10/WMOTV_TV_Infographic_JD_v2.0.jpg>. Acesso em: 6 nov. 2015.

ANEXO A – Resolução nº 510, de 7 de abril de 2016

44 ISSN 1677-7042 Diário Oficial da União - Seção 1 Nº 98, terça-feira, 24 de maio de 2016

O Plenário do Conselho Nacional de Saúde em sua Quinquagésima Nona Reunião Extraordinária, realizada nos dias 06 e 07 de abril de 2016, no uso de suas competências regimentais e atribuições conferidas pela Lei n o 8.080, de 19 de setembro de 1990, pela Lei n o 8.142, de 28 de dezembro de 1990, pelo Decreto n o 5.839, de 11 de julho de 2006, e

Considerando que a ética é uma construção humana, portanto histórica, social e cultural;

Considerando que a ética em pesquisa implica o respeito pela dignidade humana e a proteção devida aos participantes das pesquisas científicas envolvendo seres humanos;

Considerando que o agir ético do pesquisador demanda ação consciente e livre do participante;

Considerando que a pesquisa em ciências humanas e sociais exige respeito e garantia do pleno exercício dos direitos dos participantes, devendo ser concebida, avaliada e realizada de modo a prever e evitar possíveis danos aos participantes;

Considerando que as Ciências Humanas e Sociais têm especificidades nas suas concepções e práticas de pesquisa, na medida em que nelas prevalece uma acepção pluralista de ciência da qual decorre a adoção de múltiplas perspectivas teórico-metodológicas, bem como lidam com atribuições de significado, práticas e representações, sem intervenção direta no corpo humano, com natureza e grau de risco específico;

Considerando que a relação pesquisador-participante se constrói continuamente no processo da pesquisa, podendo ser redefinida a qualquer momento no diálogo entre subjetividades, implicando reflexividade e construção de relações não hierárquicas;

Considerando os documentos que constituem os pilares do reconhecimento e da afirmação da dignidade, da liberdade e da autonomia do ser humano, como a Declaração Universal dos Direitos Humanos, de 1948 e a Declaração Interamericana de Direitos e Deveres Humanos, de 1948;

Considerando a existência do sistema dos Comitês de Ética em Pesquisa e da Comissão Nacional de Ética em Pesquisa;

Considerando que a Resolução 466/12, no artigo XIII.3, reconhece as especificidades éticas das pesquisas nas Ciências Humanas e Sociais e de outras que se utilizam de metodologias próprias dessas áreas, dadas suas particularidades;

Considerando que a produção científica deve implicar benefícios atuais ou potenciais para o ser humano, para a comunidade na qual está inserido e para a sociedade, possibilitando a promoção de qualidade digna de vida a partir do respeito aos direitos civis, sociais, culturais e a um meio ambiente ecologicamente equilibrado; e

Considerando a importância de se construir um marco normativo claro, preciso e plenamente compreensível por todos os envolvidos nas atividades de pesquisa em Ciências Humanas e Sociais, resolve:

Art. 1 o Esta Resolução dispõe sobre as normas aplicáveis a pesquisas em Ciências Humanas e Sociais cujos procedimentos metodológicos envolvam a utilização de dados diretamente obtidos com os participantes ou de informações identificáveis ou que possam acarretar riscos maiores do que os existentes na vida cotidiana, na forma definida nesta Resolução.

Parágrafo único. Não serão registradas nem avaliadas pelo sistema CEP/CONEP:

I - pesquisa de opinião pública com participantes não identificados;

II - pesquisa que utilize informações de acesso público, nos termos da Lei n o 12.527, de 18 de novembro de 2011;

III - pesquisa que utilize informações de domínio público;

IV - pesquisa censitária;

V - pesquisa com bancos de dados, cujas informações são agregadas, sem possibilidade de identificação individual; e

VI - pesquisa realizada exclusivamente com textos científicos para revisão da literatura científica;

VII - pesquisa que objetiva o aprofundamento teórico de situações que emergem espontânea e contingencialmente na prática profissional, desde que não revelem dados que possam identificar o sujeito; e

III - atividade realizada com o intuito exclusivamente de educação, ensino ou treinamento sem finalidade de pesquisa científica, de alunos de graduação, de curso técnico, ou de profissionais em especialização.

§ 1 o Não se enquadram no inciso antecedente os Trabalhos de Conclusão de Curso, monografias e similares, devendo-se, nestes casos, apresentar o protocolo de pesquisa ao sistema CEP/CONEP;

§ 2 o Caso, durante o planejamento ou a execução da atividade de educação, ensino ou treinamento surja a intenção de incorporação dos resultados dessas atividades em um projeto de pesquisa, dever-se-á, de forma obrigatória, apresentar o protocolo de pesquisa ao sistema CEP/CONEP.

Capítulo I

DOS TERMOS E DEFINIÇÕES

Art. 2 o Para os fins desta Resolução, adotam-se os seguintes termos e definições:

I - assentimento livre e esclarecido: anuência do participante da pesquisa - criança, adolescente ou indivíduos impedidos de forma temporária ou não de consentir, na medida de sua compreensão e respeitadas suas singularidades, após esclarecimento sobre a natureza da pesquisa, justificativa, objetivos, métodos, potenciais benefícios e riscos. A obtenção do assentimento não elimina a necessidade do consentimento do responsável;

II - assistência ao participante da pesquisa: é aquela prestada para atender danos imateriais decorrentes, direta ou indiretamente, da pesquisa;

III - benefícios: contribuições atuais ou potenciais da pesquisa para o ser humano, para a comunidade na qual está inserido e para a sociedade, possibilitando a promoção de qualidade digna de vida, a partir do respeito aos direitos civis, sociais, culturais e a um meio ambiente ecologicamente equilibrado;

IV - confidencialidade: é a garantia do resguardo das informações dadas em confiança e a proteção contra a sua revelação não autorizada;

V - consentimento livre e esclarecido: anuência do participante da pesquisa ou de seu representante legal, livre de simulação, fraude, erro ou intimidação, após esclarecimento sobre a natureza da pesquisa, sua justificativa, seus objetivos, métodos, potenciais benefícios e riscos;

VI - informações de acesso público: dados que podem ser utilizados na produção de pesquisa e na transmissão de conhecimento e que se encontram disponíveis sem restrição ao acesso dos pesquisadores e dos cidadãos em geral, não estando sujeitos a limitações relacionadas à privacidade, à segurança ou ao controle de acesso. Essas informações podem estar processadas, ou não, e contidas em qualquer meio, suporte e formato produzido ou gerido por órgãos públicos ou privados;

VII - dano material: lesão que atinge o patrimônio do participante da pesquisa em virtude das características ou dos resultados do processo de pesquisa, impondo uma despesa pecuniária ou diminuindo suas receitas auferidas ou que poderiam ser auferidas;

VIII - dano imaterial: lesão em direito ou bem da personalidade, tais como integridades física e psíquica, saúde, honra, imagem, e privacidade, ilicitamente produzida ao participante da pesquisa por características ou resultados do processo de pesquisa;

IX - discriminação: caracterização ou tratamento social de uma pessoa ou grupo de pessoas, com consequente violação da dignidade humana, dos direitos humanos e sociais e das liberdades fundamentais dessa pessoa ou grupo de pessoas;

X - esclarecimento: processo de apresentação clara e acessível da natureza da pesquisa, sua justificativa, seus objetivos, métodos, potenciais benefícios e riscos, concebido na medida da compreensão do participante, a partir de suas características individuais, sociais, econômicas e culturais, e em razão das abordagens metodológicas aplicadas. Todos esses elementos determinam se o esclarecimento dar-se-á por documento escrito, por imagem ou de forma oral, registrada ou sem registro;

XI - estigmatização: atribuição de conteúdo negativo a uma ou mais características (estigma) de uma pessoa ou grupo de pessoas, com consequente violação à dignidade humana, aos direitos humanos e liberdades fundamentais dessa pessoa ou grupo de pessoas;

XII - etapas preliminares de uma pesquisa: são assim consideradas as atividades que o pesquisador tem que desenvolver para averiguar as condições de possibilidade de realização da pesquisa, incluindo investigação documental e contatos diretos com possíveis participantes, sem sua identificação e sem o registro público e formal das informações assim obtidas; não devendo ser confundidas com "estudos exploratórios" ou com "pesquisas piloto", que devem ser consideradas como projetos de pesquisas. Incluem-se nas etapas preliminares as visitas às comunidades, aos serviços, as conversas com liderança comunitárias, entre outros;

XIII - participante da pesquisa: indivíduo ou grupo, que não sendo membro da equipe de pesquisa, dela participa de forma esclarecida e voluntária, mediante a concessão de consentimento e também, quando couber, de assentimento, nas formas descritas nesta resolução;

XIV - pesquisa de opinião pública: consulta verbal ou escrita de caráter pontual, realizada por meio de metodologia específica, através da qual o participante, é convidado a expressar sua preferência, avaliação ou o sentido que atribui a temas, atuação de pessoas e organizações, ou a produtos e serviços; sem possibilidade de identificação do participante;

XV - pesquisa encoberta: pesquisa conduzida sem que os participantes sejam informados sobre objetivos e procedimentos do estudo, e sem que seu consentimento seja obtido previamente ou durante a realização da pesquisa. A pesquisa encoberta somente se justifica em circunstâncias nas quais a informação sobre objetivos e procedimentos alteraria o comportamento alvo do estudo ou quando a utilização deste método se apresenta como única forma de condução do estudo, devendo ser explicitado ao CEP o procedimento a ser

Fonte: Portal ABANT (2016).

Nº 98, terça-feira, 24 de maio de 2016 Diário Oficial da União - Seção 1 ISSN 1677-7042 45

adotado pelo pesquisador com o participante, no que se refere aos riscos, comunicação ao participante e uso dos dados coletados, além do compromisso ou não com a confidencialidade. Sempre que se mostre factível, o consentimento dos participantes deverá ser buscado posteriormente;

XVI - pesquisa em ciências humanas e sociais: aquelas que se voltam para o conhecimento, compreensão das condições, existência, vivência e saberes das pessoas e dos grupos, em suas relações sociais, institucionais, seus valores culturais, suas ordenações históricas e políticas e suas formas de subjetividade e comunicação, de forma direta ou indireta, incluindo as modalidades de pesquisa que envolvam intervenção;

XVII - pesquisador responsável: pessoa com no mínimo título de tecnólogo, bacharel ou licenciatura, responsável pela coordenação e realização da pesquisa e pela integridade e bem estar dos participantes no processo de pesquisa. No caso de discentes de graduação que realizam pesquisas para a elaboração do Trabalho de Conclusão de Curso, a pesquisa será registrada no CEP, sob-responsabilidade do respectivo orientador do TCC;

XVIII - preconceito: valor negativo atribuído a uma pessoa ou grupo de pessoas, com consequente violação dos direitos civis e políticos e econômicos, sociais e culturais;

XIX - privacidade: direito do participante da pesquisa de manter o controle sobre suas escolhas e informações pessoais e de resguardar sua intimidade, sua imagem e seus dados pessoais, sendo uma garantia de que essas escolhas de vida não sofrerão invasões indevidas, pelo controle público, estatal ou não estatal, e pela reprovação social a partir das características ou dos resultados da pesquisa;

XX - processo de consentimento e de assentimento: processo pautado na construção de relação de confiança entre pesquisador e participante da pesquisa, em conformidade com sua cultura e continuamente aberto ao diálogo e ao questionamento, não sendo o registro de sua obtenção necessariamente escrito;

XXI - protocolo de pesquisa: conjunto de documentos contemplando a folha de rosto e o projeto de pesquisa com a descrição da pesquisa em seus aspectos fundamentais e as informações relativas ao participante da pesquisa, à qualificação dos pesquisadores e a todas as instâncias responsáveis. Aplica-se o disposto na norma operacional do CNS em vigor ou outra que venha a substituí-la, no que couber e quando não houver prejuízo no estabelecido nesta Resolução;

XXII - registro do consentimento ou do assentimento: documento em qualquer meio, formato ou mídia, como papel, áudio, filmagem, mídia eletrônica e digital, que registra a concessão de consentimento ou de assentimento livre e esclarecido, sendo a forma de registro escolhida a partir das características individuais, sociais, linguísticas, econômicas e culturais do participante da pesquisa e em razão das abordagens metodológicas aplicadas;

XXIII - relatório final: é aquele apresentado no encerramento da pesquisa, contendo todos os seus resultados;

XXIV - ressarcimento: compensação material dos gastos decorrentes da participação na pesquisa, ou seja, despesas do participante e seus acompanhantes, tais como transporte e alimentação;

XXV - risco da pesquisa: possibilidade de danos à dimensão física, psíquica, moral, intelectual, social, cultural do ser humano, em qualquer etapa da pesquisa e dela decorrente; e

XXVI - vulnerabilidade: situação na qual pessoa ou grupo de pessoas tenha reduzida a capacidade de tomar decisões e opor resistência na situação da pesquisa, em decorrência de fatores individuais, psicológicos, econômicos, culturais, sociais ou políticos.

Capítulo II

Capítulo II

DOS PRINCÍPIOS ÉTICOS DAS PESQUISAS EM CIÊNCIAS HUMANAS E SOCIAIS

Art. 3 o São princípios éticos das pesquisas em Ciências Humanas e Sociais:

I - reconhecimento da liberdade e autonomia de todos os envolvidos no processo de pesquisa, inclusive da liberdade científica e acadêmica;

II - defesa dos direitos humanos e recusa do arbítrio e do autoritarismo nas relações que envolvem os processos de pesquisa;

III - respeito aos valores culturais, sociais, morais e religiosos, bem como aos hábitos e costumes, dos participantes das pesquisas;

IV - empenho na ampliação e consolidação da democracia por meio da socialização da produção de conhecimento resultante da pesquisa, inclusive em formato acessível ao grupo ou população que foi pesquisada;

V - recusa de todas as formas de preconceito, incentivando o respeito à diversidade, à participação de indivíduos e grupos vulneráveis e discriminados e às diferenças dos processos de pesquisa;

VI - garantia de assentimento ou consentimento dos participantes das pesquisas, esclarecidos sobre seu sentido e implicações;

VII - garantia da confidencialidade das informações, da privacidade dos participantes e da proteção de sua identidade, inclusive do uso de sua imagem e voz;

VIII - garantia da não utilização, por parte do pesquisador, das informações obtidas em pesquisa em prejuízo dos seus participantes;

IX - compromisso de todos os envolvidos na pesquisa de não criar, manter ou ampliar as situações de risco ou vulnerabilidade para indivíduos e coletividades, nem acentuar o estigma, o preconceito ou a discriminação; e

X - compromisso de propiciar assistência a eventuais danos materiais e imateriais, decorrentes da participação na pesquisa, conforme o caso sempre e enquanto necessário.

Capítulo III

DO PROCESSO DE CONSENTIMENTO E DO ASSENTIMENTO LIVRE E ESCLARECIDO

Art. 4 o O processo de consentimento e do assentimento livre e esclarecido envolve o estabelecimento de relação de confiança entre pesquisador e participante, continuamente aberto ao diálogo e ao questionamento, podendo ser obtido ou registrado em qualquer das fases de execução da pesquisa, bem como retirado a qualquer momento, sem qualquer prejuízo ao participante.

Art. 5 o O processo de comunicação do consentimento e do assentimento livre e esclarecido pode ser realizado por meio de sua expressão oral, escrita, língua de sinais ou de outras formas que se mostrem adequadas, devendo ser consideradas as características individuais, sociais, econômicas e culturais da pessoa ou grupo de pessoas participante da pesquisa e as abordagens metodológicas aplicadas.

§ 1 o O processo de comunicação do consentimento e do assentimento livre e esclarecido deve ocorrer de maneira espontânea, clara e objetiva, e evitar modalidades excessivamente formais, num clima de mútua confiança, assegurando uma comunicação plena e interativa.

§ 2 o No processo de comunicação do consentimento e do assentimento livre e esclarecido, o participante deverá ter a oportunidade de esclarecer suas dúvidas, bem como dispor do tempo que lhe for adequado para a tomada de uma decisão autônoma.

Art. 6 o O pesquisador deverá buscar o momento, condição e local mais adequado para que os esclarecimentos sobre a pesquisa sejam efetuados, considerando, para isso, as peculiaridades do convidado a participar da pesquisa, a quem será garantido o direito de recusa.

Art. 7 o O pesquisador deverá assegurar espaço para que o participante possa expressar seus receios ou dúvidas durante o processo de pesquisa, evitando qualquer forma de imposição ou constrangimento, respeitando sua cultura.

Art. 8 o As informações sobre a pesquisa devem ser transmitidas de forma acessível e transparente para que o convidado a participar de uma pesquisa, ou seu representante legal, possa se manifestar, de forma autônoma, consciente, livre e esclarecida.

Art. 9 o São direitos dos participantes:

I - ser informado sobre a pesquisa;

II - desistir a qualquer momento de participar da pesquisa, sem qualquer prejuízo;

III - ter sua privacidade respeitada;

IV - ter garantida a confidencialidade das informações pessoais;

V - decidir se sua identidade será divulgada e quais são, dentre as informações que forneceu, as que podem ser tratadas de forma pública;

VI - ser indenizado pelo dano decorrente da pesquisa, nos termos da Lei; e

VII - o ressarcimento das despesas diretamente decorrentes de sua participação na pesquisa.

Seção I

Da obtenção do Consentimento e do Assentimento

Art. 10. O pesquisador deve esclarecer o potencial participante, na medida de sua compreensão e respeitadas suas singularidades, sobre a natureza da pesquisa, seus objetivos, métodos, direitos, riscos e potenciais benefícios.

Art. 11. O consentimento do participante da pesquisa deverá ser particularmente garantido àquele que, embora plenamente capaz, esteja exposto a condicionamentos específicos, ou sujeito a relação de autoridade ou de dependência, caracterizando situações passíveis de limitação da autonomia.

limitação da autonomia.

Art. 12. Deverá haver justificativa da escolha de crianças, de adolescentes e de pessoas em situação de diminuição de sua capacidade de decisão no protocolo a ser aprovado pelo sistema CEP/CONEP.

Parágrafo único. Nos casos previstos no caput deverão ser obtidos o assentimento do participante e o consentimento livre e esclarecido, por meio dos representantes legais do participante da pesquisa, preservado o direito à informação e à autonomia do participante, de acordo com a sua capacidade.

Art. 13. Em comunidades cuja cultura reconheça a autoridade do líder ou do coletivo sobre o indivíduo, como é o caso de algumas comunidades tradicionais, indígenas ou religiosas, por exemplo, a obtenção da autorização para a pesquisa deve respeitar tal particularidade, sem prejuízo do consentimento individual, quando possível e desejável.

Art. 14. Quando for inviável a realização do processo de Consentimento Livre e Esclarecido, a dispensa desse processo deve ser justificadamente solicitada pelo pesquisador responsável ao Sistema CEP/CONEP para apreciação.

Seção II

Do Registro do Consentimento e do Assentimento

Art. 15. O Registro do Consentimento e do Assentimento é o meio pelo qual é explicitado o consentimento livre e esclarecido do participante ou de seu responsável legal, sob a forma escrita, sonora, imagética, ou em outras formas que atendam às características da pesquisa e dos participantes, devendo conter informações em linguagem clara e de fácil entendimento para o suficiente esclarecimento sobre a pesquisa.

§ 1º Quando não houver registro de consentimento e do assentimento, o pesquisador deverá entregar documento ao participante que contemple as informações previstas para o consentimento livre e esclarecido sobre a pesquisa.

§ 2º A obtenção de consentimento pode ser comprovada também por meio de testemunha que não componha a equipe de pesquisa e que acompanhou a manifestação do consentimento.

Art. 16. O pesquisador deverá justificar o meio de registro mais adequado, considerando, para isso, o grau de risco envolvido, as características do processo da pesquisa e do participante.

§ 1º Os casos em que seja inviável o Registro de Consentimento ou do Assentimento Livre e Esclarecido ou em que este registro signifique riscos substanciais à privacidade e confidencialidade dos dados do participante ou aos vínculos de confiança entre pesquisador e pesquisado, a dispensa deve ser justificada pelo pesquisador responsável ao sistema CEP/CONEP.

§ 2º A dispensa do registro de consentimento ou de assentimento não isenta o pesquisador do processo de consentimento ou de assentimento, salvo nos casos previstos nesta Resolução.

§ 3º A dispensa do Registro do Consentimento deverá ser avaliada e aprovada pelo sistema CEP/CONEP.

Art. 17. O Registro de Consentimento Livre e Esclarecido, em seus diferentes formatos, deverá conter esclarecimentos suficientes sobre a pesquisa, incluindo:

I - a justificativa, os objetivos e os procedimentos que serão utilizados na pesquisa, com informação sobre métodos a serem utilizados, em linguagem clara e acessível, aos participantes da pesquisa, respeitada a natureza da pesquisa;

II - a explicitação dos possíveis danos decorrentes da participação na pesquisa, além da apresentação das providências e cautelas a serem empregadas para evitar situações que possam causar dano, considerando as características do participante da pesquisa;

III - a garantia de plena liberdade do participante da pesquisa para decidir sobre sua participação, podendo retirar seu consentimento, em qualquer fase da pesquisa, sem prejuízo algum;

IV - a garantia de manutenção do sigilo e da privacidade dos participantes da pesquisa seja pessoa ou grupo de pessoas, durante todas as fases da pesquisa, exceto quando houver sua manifestação explícita em sentido contrário, mesmo após o término da pesquisa;

V - informação sobre a forma de acompanhamento e a assistência a que terão direito os participantes da pesquisa, inclusive considerando benefícios, quando houver;

VI - garantia aos participantes do acesso aos resultados da pesquisa;

VII - explicitação da garantia ao participante de ressarcimento e a descrição das formas de cobertura das despesas realizadas pelo participante decorrentes da pesquisa, quando houver;

VIII - a informação do endereço, e-mail e contato telefônico, dos responsáveis pela pesquisa;

IX - breve explicação sobre o que é o CEP, bem como endereço, e-mail e contato telefônico do CEP local e, quando for o caso, da CONEP; e

X - a informação de que o participante terá acesso aos registros do consentimento sempre que solicitado.

§ 1 o Nos casos em que algum dos itens não for contemplado na modalidade de registro escolhida, tal informação deverá ser entregue ao participante em documento complementar, de maneira a garantir que todos os itens supracitados sejam informados aos participantes.

§ 2 o Nos casos em que o consentimento ou o assentimento livre e esclarecido não for registrado por escrito, o participante poderá ter acesso ao registro do consentimento ou do assentimento sempre que solicitado.

§ 3 o Nos casos em que o consentimento ou o assentimento livre e esclarecido for registrado por escrito uma via, assinada pelo participante e pelo pesquisador responsável, deve ser entregue ao participante.

§ 4 o O assentimento do participante da pesquisa deverá constar do registro do consentimento.

Capítulo IV

Capítulo IV

DOS RISCOS

Art. 18. Nos projetos de pesquisa em Ciências Humanas e Sociais, a definição e a gradação do risco resultam da apreciação dos seus procedimentos metodológicos e do seu potencial de causar danos maiores ao participante do que os existentes na vida cotidiana, em consonância com o caráter processual e dialogal dessas pesquisas.

Art. 19. O pesquisador deve estar sempre atento aos riscos que a pesquisa possa acarretar aos participantes em decorrência dos seus procedimentos, devendo para tanto serem adotadas medidas de precaução e proteção, a fim de evitar dano ou atenuar seus efeitos.

§ 1 o Quando o pesquisador perceber qualquer possibilidade de dano ao participante, decorrente da participação na pesquisa, deverá discutir com os participantes as providências cabíveis, que podem incluir o encerramento da pesquisa e informar o sistema CEP/CONEP.

§ 2 o O participante da pesquisa que vier a sofrer qualquer tipo de dano resultante de sua participação na pesquisa, previsto ou não no Registro de Consentimento Livre e Esclarecido, tem direito a assistência e a buscar indenização.

Art. 20. O pesquisador deverá adotar todas as medidas cabíveis para proteger o participante quando criança, adolescente, ou qualquer pessoa cuja autonomia esteja reduzida ou que esteja sujeita a relação de autoridade ou dependência que caracterize situação de limitação da autonomia, reconhecendo sua situação peculiar de vulnerabilidade, independentemente do nível de risco da pesquisa.

Art. 21. O risco previsto no protocolo será graduado nos níveis mínimo, baixo, moderado ou elevado, considerando sua magnitude em função de características e circunstâncias do projeto, conforme definição de Resolução específica sobre tipificação e gradação de risco e sobre tramitação dos protocolos.

§ 1 o A tramitação dos protocolos será diferenciada de acordo com a gradação de risco.

§ 2 o A gradação do risco deve distinguir diferentes níveis de precaução e proteção em relação ao participante da pesquisa.

Fonte: Portal ABANT (2016).

46 ISSN 1677-7042 Diário Oficial da União - Seção 1 Nº 98, terça-feira, 24 de maio de 2016

Capítulo V
DO PROCEDIMENTO DE ANÁLISE ÉTICA NO SISTEMA CEP/CONEP
Art. 22. O protocolo a ser submetido à avaliação ética somente será apreciado se for apresentada toda a documentação solicitada pelo sistema CEP/CONEP, tal como descrita, a esse respeito, na norma operacional do CNS em vigor, no que couber e quando não houver prejuízo no estabelecido nesta Resolução, considerando a natureza e as especificidades de cada pesquisa.
Art. 23. Os projetos de pesquisa serão inscritos na Plataforma Brasil, para sua avaliação ética, da forma prevista nesta Resolução e na Resolução específica de gradação, tipificação de risco e tramitação dos protocolos.
Art. 24. Todas as etapas preliminares necessárias para que o pesquisador elabore seu projeto não são alvo de avaliação do sistema CEP/CONEP.
Art. 25. A avaliação a ser feita pelo Sistema CEP/CONEP incidirá sobre os aspectos éticos dos projetos, considerando os riscos e a devida proteção dos direitos dos participantes da pesquisa.
§1 o . A avaliação científica dos aspectos teóricos dos projetos submetidos a essa Resolução compete às instâncias acadêmicas específicas, tais como comissões acadêmicas de pesquisa, bancas de pós-graduação, instituições de fomento à pesquisa, dentre outros. Não cabe ao Sistema CEP/CONEP a análise do desenho metodológico em si.
§ 2 o . A avaliação a ser realizada pelo Sistema CEP/CONEP incidirá somente sobre os procedimentos metodológicos que impliquem em riscos aos participantes.
Art. 26. A análise ética dos projetos de pesquisa de que trata esta Resolução só poderá ocorrer nos Comitês de Ética em Pesquisa que comportarem representação equânime de membros das Ciências Humanas e Sociais, devendo os relatores serem escolhidos dentre os membros qualificados nessa área de conhecimento.
Art. 27. A pesquisa realizada por alunos de graduação e de pós-graduação, que seja parte de projeto do orientador já aprovado pelo sistema CEP/Conep, pode ser apresentada como emenda ao projeto aprovado, desde que não contenha modificação essencial nos objetivos e na metodologia do projeto original.
Capítulo VI
DO PESQUISADOR RESPONSÁVEL
Art. 28. A responsabilidade do pesquisador é indelegável e indeclinável e compreende os aspectos éticos e legais, cabendo-lhe:
I - apresentar o protocolo devidamente instruído ao sistema CEP/Conep, aguardando a decisão de aprovação ética, antes de iniciar a pesquisa, conforme definido em resolução específica de tipificação e gradação de risco;
II - conduzir o processo de Consentimento e de Assentimento Livre e Esclarecido;
III - apresentar dados solicitados pelo CEP ou pela Conep a qualquer momento;
IV - manter os dados da pesquisa em arquivo, físico ou digital, sob sua guarda e responsabilidade, por um período mínimo de 5 (cinco) anos após o término da pesquisa; e
V - apresentar no relatório final que o projeto foi desenvolvido conforme delineado, justificando, quando ocorridas, a sua mudança ou interrupção.
Capítulo VII
DAS DISPOSIÇÕES TRANSITÓRIAS
Art. 29. Será instituída instância, no âmbito da Conep, para implementação, acompanhamento, proposição de atualização desta Resolução e do formulário próprio para inscrição dos protocolos relativos a projetos das Ciências Humanas e Sociais na Plataforma Brasil, bem como para a proposição de projetos de formação e capacitação na área.
Parágrafo único. A instância prevista no caput será composta por membros titulares das Ciências Humanas e Sociais integrantes da CONEP, representantes das associações científicas nacionais de Ciências Humanas e Sociais, membros dos CEP de Ciências Humanas e Sociais e de usuários.
Art. 30. Deverá ser estimulado o ingresso de pesquisadores e demais profissionais atuantes nas Ciências Humanas e Sociais nos colegiados dos CEP existentes, assim como a criação de novos CEP, mantendo-se a interdisciplinaridade em sua composição.
Art. 31. Os aspectos relacionados às modificações necessárias na Plataforma Brasil entrarão em vigor quando da atualização do sistema.
Capítulo VIII
DAS DISPOSIÇÕES FINAIS
Art. 32. Aplica-se o disposto nos itens VII, VIII, IX e X, da Resolução CNS n o 466, de 12, de dezembro de 2012, no que couber e quando não houver prejuízo ao disposto nesta Resolução.
Parágrafo único. Em situações não contempladas por essa Resolução, prevalecerão os princípios éticos contidos na Resolução CNS n o 466 de 2012.
Art. 33. A composição da Conep respeitará a equidade dos membros titulares e suplentes indicados pelos CEP entre a área de Ciências Humanas e Sociais e as demais áreas que a compõem, garantindo a representação equilibrada das diferentes áreas na elaboração de normas e no gerenciamento do Sistema CEP/CONEP.
Art. 34. Esta Resolução entra em vigor na data de sua publicação.

RONALD FERREIRA DOS SANTOS
Presidente do Conselho Nacional de Saúde

Homologo a Resolução CNS nº 510, de 7 de abril de 2016, nos termos do Decreto de Delegação de Competência de 12 de novembro de 1991.

MARCELO CASTRO
Ministro de Estado da Saúde

SECRETARIA DE ATENÇÃO À SAÚDE

PORTARIA Nº 597, DE 23 DE MAIO DE 2016

Habilita o Hospital Oswaldo Cruz como Unidade de Assistência em Alta Complexidade no Tratamento da Lipoatrofia Facial do Portador de HIV/AIDS.

A Secretária de Atenção à Saúde - Substituta, no uso de suas atribuições,
Considerando a Portaria nº 2.582/GM/MS, de 02 de dezembro de 2004, que inclui cirurgias reparadoras para pacientes portadores de AIDS e usuários de anti-retrovirais;
Considerando a Portaria SAS/SVS/MS nº 01 de 20 de janeiro de 2009, que trata das normas para habilitação/credenciamento dos Serviços de Tratamento da Lipodistrofia do Portador de HIV/AIDS e Serviços de Tratamento da Lipoatrofia Facial do Portador de HIV/AIDS;
Considerando a Portaria nº 04/SAS/MS, de 20 de janeiro de 2009, que trata da operacionalização dos procedimentos referentes a cirurgias reparadoras para pacientes portadores de HIV/AIDS nos sistemas de informações do Sistema Único de Saúde - SIA e SIH;
Considerando a Portaria nº. 116/GM/MS, de 22 de janeiro de 2009, que estabelece recursos a serem incorporados ao Teto Financeiro Anual de Média e Alta Complexidade aos Estados, Distrito Federal e Municípios, para o custeio dos procedimentos referentes às cirurgias reparadoras para pacientes portadores de AIDS e usuários de anti-retrovirais;
Considerando a manifestação favorável da Secretaria de Estado da Saúde do Paraná e aprovação da habilitação pela Comissão Intergestores Bipartite do Estado, conforme as Deliberações nº 013, de 28/01/2015 e nº 195, de 03/12/2015; e
Considerando a avaliação da Unidade de Assistência e Tratamento do Programa Nacional DST-AIDS/SVS e da Coordenação Geral de Média e Alta Complexidade/DAET/SAS/MS, resolve:
Art. 1º Fica habilitado, no estado do Paraná, como Unidade de Assistência em Alta Complexidade no Tratamento da Lipoatrofia Facial do Portador de HIV/AIDS, o estabelecimento abaixo:

CNPJ	CNES	ESTABELECIMENTO
76.416.866/0009-05	0015415	Hospital Oswaldo Cruz

Art. 2º O custeio do impacto financeiro gerado por esta habilitação deverá onerar o teto do estado ou Município de acordo com o vínculo da unidade e modalidade da gestão, considerando a Portaria nº. 116/GM/MS, de 27 de março de 2009.
Art. 3º Esta Portaria entra em vigor na data da sua publicação.

CLEUSA RODRIGUES DA SILVEIRA
BERNARDO

PORTARIA Nº 598, DE 23 DE MAIO DE 2016

Altera número de leitos da Unidade de Tratamento Intensivo Tipo II do Hospital Arcanjo São Miguel - Associação Franciscana de Assistência a Saúde - Gramado/RS.

A Secretária de Atenção à Saúde-Substituta, no uso de suas atribuições,
Considerando a Portaria nº 3.432/GM/MS, de 12 de agosto de 1998, que estabelece critérios de classificação e cadastramento para as Unidades de Tratamento Intensivo;
Considerando a Portaria nº 323/SAS/MS, de 10 de junho de 2008, que cadastrou leitos de UTI Adulto para o Hospital Arcanjo São Miguel - Gramado/RS; e
Considerando o Ofício nº 204/2016, datado de 31 de março de 2016, que solicita o descredenciamento de leitos de UTI no Hospital Arcanjo São Miguel - Gramado/RS, resolve:
Art. 1º Fica alterado o número de leitos da Unidade de Tratamento Intensivo Tipo II, do hospital a seguir relacionado:

CNES	Hospital	Nº leitos
2241153	Hospital Arcanjo São Miguel - Associação Franciscana de Assistência a Saúde - Gramado/RS	
26.01 Adulto		07

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

CLEUSA RODRIGUES DA SILVEIRA
BERNARDO

PORTARIA Nº 599, DE 23 DE MAIO DE 2016

Indefere a adesão ao Programa de Fortalecimento das Entidades Privadas Filantrópicas e das Entidades sem Fins Lucrativos que Atuam na Área da Saúde e que Participam de Forma Complementar do Sistema Único de Saúde (PROSUS), da Associação Casa Fonte da Vida, com sede em Jacarei (SP).

A Secretária de Atenção à Saúde - Substituta, no uso de suas atribuições,
Considerando a Lei nº 12.873, de 24 de outubro de 2013, que instituiu o Programa de Fortalecimento das Entidades Privadas Filantrópicas e das Entidades sem Fins Lucrativos que Atuam na Área da Saúde e que Participam de Forma Complementar do Sistema Único de Saúde (PROSUS);
Considerando a Portaria nº 3.076/GM/MS de 12 de dezembro de 2013, que delega competência ao Secretário de Atenção à Saúde para execução do PROSUS;
Considerando a Portaria GM/MS nº 535, de 8 de abril de 2014, que estabelece normas para a execução no âmbito do Ministério da Saúde, do PROSUS, de que trata a Lei nº 12.873, de 24 de outubro de 2013;
Considerando a avaliação da instituição financeira oficial federal que contraindica a viabilidade do Plano de Recuperação Econômica e Financeira da entidade nos termos do art. 42 da Lei 12.873/2013;
Considerando a Adesão ao PROSUS deferida, sob condição resolutiva, da Associação Casa Fonte da Vida, CNPJ nº 50.460.351/0001-53; e
Considerando o Parecer Técnico nº 74/2016-CGAGPS/DCEBAS/SAS/MS e o Despacho nº 72/2016/DCEBAS/SAS/MS, constantes do Processo nº 25000.121098/2014-72/MS, que concluíram pelo não atendimento do requisito disposto no inciso II do art. 29 da Lei nº 12.873, de 24 de outubro de 2013, resolve:
Art. 1º Fica indeferida a adesão ao Programa de Fortalecimento das Entidades Privadas Filantrópicas e das Entidades sem Fins Lucrativos que Atuam na Área da Saúde e que Participam de Forma Complementar do Sistema Único de Saúde (PROSUS), da Associação Casa Fonte da Vida, CNPJ nº 50.460.351/0001-53, com sede em Jacarei (SP).
Art. 2º A instituição requerente fica notificada para, caso queira, apresentar recurso administrativo no prazo de 30 (trinta) dias a contar da data da presente publicação, conforme prevê o § 3º do art. 30 da Lei nº 12.873/2013.
Art. 3º Esta Portaria entra em vigor na data de sua publicação.

CLEUSA RODRIGUES DA SILVEIRA
BERNARDO

PORTARIA Nº 600, DE 23 DE MAIO DE 2016

Indefere a adesão ao Programa de Fortalecimento das Entidades Privadas Filantrópicas e das Entidades sem Fins Lucrativos que Atuam na Área da Saúde e que Participam de Forma Complementar do Sistema Único de Saúde (PROSUS), da Associação dos Funcionários Municipais de Porto Alegre, com sede em Porto Alegre (RS).

A Secretária de Atenção à Saúde - Substituta, no uso de suas atribuições,
Considerando a Lei nº 12.873, de 24 de outubro de 2013, que instituiu o Programa de Fortalecimento das Entidades Privadas Filantrópicas e das Entidades sem Fins Lucrativos que Atuam na Área da Saúde e que Participam de Forma Complementar do Sistema Único de Saúde (PROSUS);
Considerando a Portaria nº 3.076/GM/MS, de 12 de dezembro de 2013, que delega competência ao Secretário de Atenção à Saúde para execução do PROSUS;
Considerando a Portaria nº 535/GM/MS, de 8 de abril de 2014, que estabelece normas para a execução no âmbito do Ministério da Saúde, do PROSUS, de que trata a Lei nº 12.873, de 24 de outubro de 2013;
Considerando a avaliação da instituição financeira oficial federal que contraindica a viabilidade do Plano de Recuperação Econômica e Financeira da entidade nos termos do art. 42 da Lei 12.873/2013;
Considerando a adesão ao PROSUS deferida, sob condição resolutiva, da Associação dos Funcionários Municipais de Porto Alegre, CNPJ nº 92.831.163/0001-34; e
Considerando o Parecer Técnico nº 78/2016-CGAGPS/DCEBAS/SAS/MS e o Despacho nº 74/2016/DECEBAS/SAS/MS, constantes do processo nº 25000.119365/2014-41/MS, que concluíram que a entidade não atende ao requisito do inciso II do art. 29 da Lei nº 12.873, de 24 de outubro de 2013, resolve:
Art. 1º Fica indeferido a adesão ao Programa de Fortalecimento das Entidades Privadas Filantrópicas e das Entidades sem Fins Lucrativos que Atuam na Área da Saúde e que Participam de Forma Complementar do Sistema Único de Saúde (PROSUS), da Associação dos Funcionários Municipais de Porto Alegre, CNPJ nº 92.831.163/0001-34, com sede em Porto Alegre (RS).

Fonte: Portal ABANT (2016).

ANEXO – B

ERRATA

MARIO CESAR. P.PEIXOTO, de. Interdisciplinar em Tecnologias, Comunicação e Educação. 2016. 131 f. Dissertação (Mestrado Profissional) — Universidade Federal de Uberlândia, 2017.

Folha	Linha	Onde se lê	Leia-se
86	3	de forma que a ferramenta realiza o cálculo da média final com uma visão interna e externa para cada elemento	de forma que a ferramenta realiza o cálculo da média final com uma visão interna e externa para cada elemento, vale complementar com relação à matriz SWOT, explicitando os parâmetros utilizados para avaliar as situações/características (que foram seis) e notas (que vão de 1 a 5): ○ As 6 (seis) principais situações/características elucidadas, foram designadas pelo próprio autor, de maneira que prevalecem com quesitos considerados para esta elaboração a situação mercadológica, econômica, social e cultural no pais. ○ As notas avaliadas entre 1 à 5, foram designadas pelo próprio autor considerando sua percepção e experiência profissional e de mercado.

88	6	onde se pode visualizar facilmente quais itens têm maior prioridade em relação aos demais	onde se pode visualizar facilmente quais itens têm maior prioridade em relação aos demais, vale complementar com relação à matriz GUT, sobre a forma como foi avaliada a prioridade: ○ A prioridade se dá pela soma dos campos de analise: GRAVIDADE + URGÊNCIA + TENDÊNCIA. De modo que cada campo de analise (que variam numa ponderação de 1 a 5), foram designados pela avaliação/analise do próprio autor, mediante suas percepções e experiências nos quesitos referentes a cada problema destacados na figura 22, na qual conseguiu-se responder as três principais perguntas (O QUE, PORQUE, POR ONDE).
107	16		Com relação aos dados das figuras/gráficos referentes à Pesquisa: ○ Poderá ser acessado e melhor visualizado em: https://goo.gl/Qz07v7