Lefosse

Cartilha

Governança Digital:
O que é e por que é importante?

Maio 2024

No início da década passada, a disseminação do uso da internet e de serviços online, com destaque para o surgimento e a ampliação das redes sociais, levou o Direito Digital a ganhar força como uma ferramenta para enfrentar os novos desafios jurídicos, como aspectos regulatórios do uso da internet, responsabilidades dos agentes econômicos, direitos dos indivíduos, regulação de negócios inovadores, entre outros. Diante deste cenário, foi promulgada, após anos de discussão do público e do Congresso Nacional, em 23 de abril de 2014, a Lei nº 12.9645, conhecida como **Marco Civil da Internet**.

O Marco Civil da Internet foi idealizado como uma carta de princípios, direitos e deveres organizados com o intuito de disciplinar o uso e o funcionamento da internet no país. Na época de sua concepção, discutia-se o uso e a prestação de serviços de internet, principalmente sob a lógica de se regular a atuação de provedores de serviços de internet, divididos pelo legislador em "provedores de conexão" e "provedores de aplicação".

Contudo, a última década testemunhou a aceleração exponencial na digitalização de serviços, inclusive em organizações de diversos setores da economia, com uma verdadeira migração para o ambiente virtual de muitas atividades que antes eram majoritariamente realizadas "off-line". Este movimento foi também impulsionado pela pandemia global de COVID-19, que provocou uma transformação digital forçada, trazendo para o universo "online" jornadas de trabalho, hábitos de consumo, obtenção de conhecimento e educação, serviços de saúde, entre outros. Além disso, tal fenômeno ganhou ainda maior relevância com o rápido desenvolvimento de sistemas de Inteligência Artificial (IA), sobretudo a IA generativa, nos últimos dois anos.

Desse modo, testemunhamos na última década a evolução para um cenário econômico fortemente baseado no uso de tecnologias, dados e internet por entidades dos mais diversos setores, de modo que a preocupação com questões relacio-

nadas ao Direito Digital deixou de ser uma exclusividade das "empresas de tecnologia" e passou a integrar a estrutura de organizações de todos os setores. Faz sentido, portanto, tratar do conceito abrangente de **Governança Digital**, que engloba o conjunto de processos e políticas voltados à gestão e ao uso estratégico das tecnologias digitais, adaptados aos distintos graus de transformação digital de cada organização.

Para além do gerenciamento dos recursos tecnológicos e do cumprimento de obrigações legais, a Governança Digital contempla a definição de estratégias para o uso responsável e ético de tecnologias e da internet, a mitigação de riscos de segurança cibernética, a proteção de dados, a aderência a normas e padrões relevantes aplicáveis à atividade econômica, a proteção de ativos de propriedade intelectual, dentre outros temas.

Assim, à medida que a tecnologia da informação desempenha papel central em diversas organizações – sejam elas do setor de tecnologia ou não –, a Governança Digital ganha relevância estratégica por garantir que estas aproveitem ao máximo os benefícios da tecnologia disponível para aprimorar a eficiência de seus negócios, ao mesmo tempo em que gerenciam adequadamente os riscos associados ao seu uso.

Esta cartilha, portanto, perpassa por diversos temas a serem englobados na implementação jurídica de uma estrutura integrada de Governança Digital, abrangendo temas relacionados a diversos ramos do direito além do Direito Digital, tais como como Propriedade Intelectual, Societário, Tributário e Trabalhista.

Sumário

Lefosse

1 Compliance de plataformas digitais

A prestação de serviços ou oferecimento de produtos por meio de plataformas digitais — i.e., *sites*, aplicativos móveis, redes sociais, *e-commerce*, *marketplaces*, entre outros —, ou mesmo o desenvolvimento de plataformas digitais para otimização de processos internos, é um elemento presente na estratégia digital de diversas organizações.

No contexto atual, é essencial que as plataformas digitais não apenas cumpram com as obrigações legais estabelecidas pelo Marco Civil da Internet e pela Lei n. 13.709/2018 ("**LGPD**"), mas também considerem outras normas que possam influenciar suas atividades em meio digital. Assim, é fundamental a implementação de medidas efetivas de Governança Digital para mitigar riscos jurídicos e fomentar a confiança de *stakeholders*.

Tais medidas podem englobar, conforme as particularidades de cada plataforma:

- definição das **regras de uso e contratação da plataforma por parte do usuário**, por meio da inclusão de termos e condições de uso da plataforma, bem como de contratos de compra e venda digitais relacionados aos produtos ou serviços contratados, conforme aplicável;

- adoção de medidas visando atender às regras de **proteção de dados pessoais e privacidade**, assegurando que os dados dos usuários sejam tratados em conformidade com a legislação aplicável, incluindo, por exemplo, efetiva transparência por meio de **políticas de privacidade** e aderência às melhores práticas e recomendações da ANPD sobre **uso de tecnologias de rastreamento, como *cookies***;

- gestão de **denúncias por meio da própria plataforma e atendimento de notificações ou ordens judiciais**, de acordo com a legislação aplicável e a situação fática que gerou a solicitação, além das políticas da companhia;

- adoção de medidas de **conformidade com o Código de Defesa do Consumidor**, garantindo adequada divulgação de informações sobre produtos e serviços, políticas claras e transparentes sobre exercício do direito de arrependimento e regras de trocas, devoluções e reembolsos, além de disponibilização de serviço de atendimento ao cliente acessível e eficiente;

- adoção de medidas de **conformidade regulatória**, abrangendo obrigações aplicáveis a todas as plataformas, como as estipuladas no Marco Civil da Internet, além de obrigações específicas aplicáveis a setores regulados, por exemplo, plataformas relacionadas a serviços financeiros, saúde, educação, entretenimento etc.;

- definição da **estratégia de marketing digital** em conformidade com o Código Brasileiro de Autorregulamentação Publicitária do CONAR, além das regras aplicáveis a uso de imagem, direitos autorais, contratação de influenciadores, compra e direcionamento de anúncios pagos, promoções comerciais (como sorteios), entre outros aspectos;

- gestão da relação com vendedores, no caso de **operações de *marketplace***, incluindo implementação de ferramentas de monitoramento de conformidade com os termos de uso da plataforma (e.g., restrições à venda de produtos contrafeitos e ilícitos);

- adoção de medidas ativas e preventivas para a **proteção dos direitos das crianças e adolescentes**, em conformidade com o Estatuto da Criança e do Adolescente e outras normas aplicáveis, incluindo classificação de conteúdos de acordo com a classificação etária, procedimentos de verificação de idade dos usuários e mecanismos de controle parental;

- implementação de ferramentas de **acessibilidade na plataforma**, assegurando conformidade com o Estatuto da Pessoa com Deficiência (Lei nº 13.146/2015) e outras regras aplicáveis e padrões recomendados;

- gestão de questões relevantes envolvendo **serviços de pagamento**, incluindo contratos com fornecedores, medidas de segurança das transações, conformidade com certificações internacionais como o PCI-DSS para transações com cartões de crédito, regras de *chargeback*, sistemas antifraude, entre outros.

Dada a abrangência de temas aplicáveis às plataformas digitais, é importante que a estratégia de Governança Digital tenha o envolvimento das áreas estratégicas da organização, possibilitando a definição e a implementação de processos internos que assegurem, monitorem e mantenham a conformidade das plataformas digitais em todos os aspectos essenciais.

2 Software e Contratos de Tecnologia

A gestão eficaz dos softwares utilizados, especialmente daqueles críticos para a infraestrutura tecnológica e continuidade das operações, corresponde ao aspecto essencial da Governança Digital, independentemente do setor de atuação da organização.

O Brasil conta com lei específica para tratar da proteção aos programas de computador (softwares), a Lei nº. 9.609/98, ou "Lei de Software". Ainda assim, os termos dos contratos de software e prestação de serviços de tecnologia – por exemplo, serviços de tecnologia da informação, *outsourcing*, *collocation*, *cloud computing*, dentre outros – exercem papel importante na gestão desses ativos, na medida em que regulam os termos e condições para o desenvolvimento, implementação e suporte de sistemas e tecnologias essenciais para a infraestrutura técnica da organização e suas operações digitais.

(i) **Softwares de terceiros:** a Governança Digital neste âmbito é essencial tanto para permitir a adequada contratação de fornecedores como para garantir a vigência e o cumprimento às regras de utilização previstas em contratos de licença de software. Isto pode se dar pela criação e manutenção de um inventário abrangente de softwares e definição de boas práticas para atualizá-lo regularmente, de modo a evitar potenciais riscos decorrentes de violações de licença.

Assim, além da adequada gestão interna de contratos, uma boa Governança Digital em software e contratos de tecnologia pode englobar, dentre outras, as seguintes atividades:

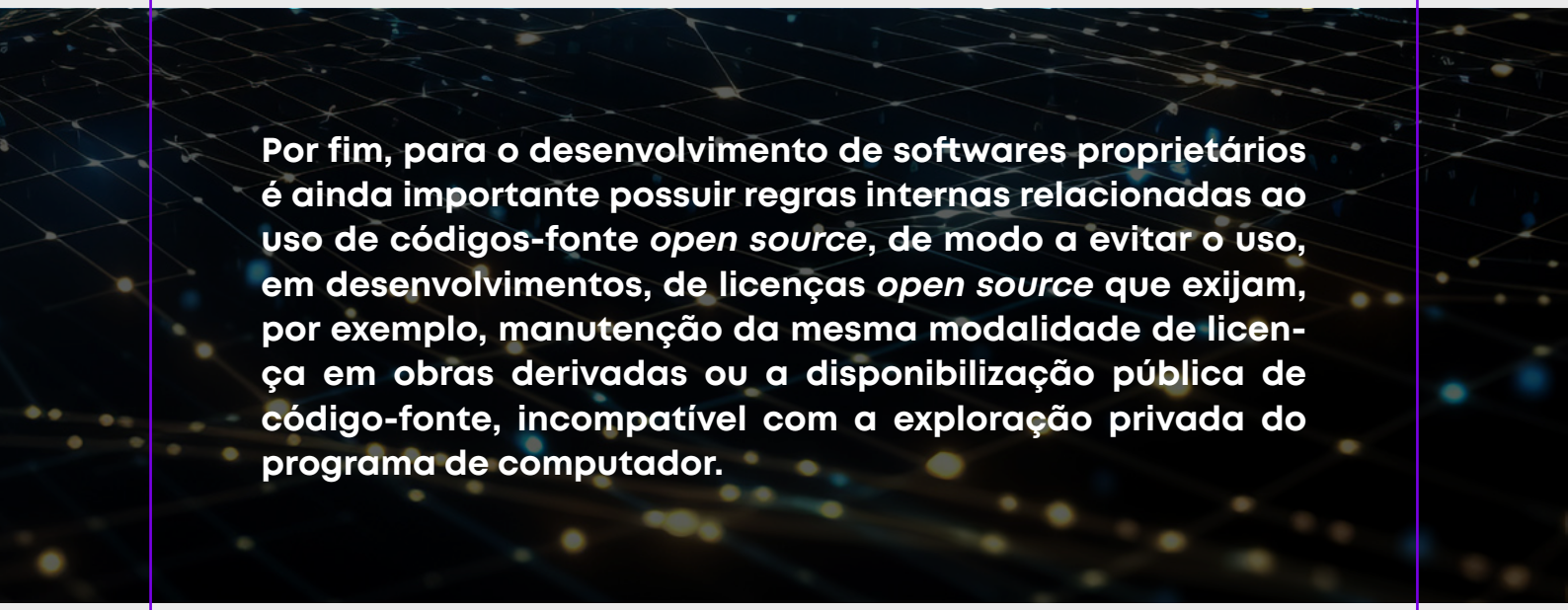
- realização de procedimentos adequados de concorrência (*request for proposals* – RFPs) para a contratação de licenças de software ou de outros fornecedores de tecnologia, visando, desde o início do processo, estabelecer de forma clara as necessidades da organização e as expectativas com relação ao fornecedor;
- negociação de contratos de licença de software e/ou fornecimento de tecnologia alinhados às necessidades e interesses da organização, considerando aspectos como métricas de uso das licenças, eventuais custos "invisíveis", limitações de indenização, regras para rescisão, legislação aplicável, dentre outros fatores;
- condução de auditorias em fornecedor de tecnologia, para, por exemplo, confirmar o atendimento a padrões de segurança da informação requeridos pela organização;

- procedimentos para lidar com auditorias de fornecedores de software, bem como para analisar e responder a eventuais apontamentos de uso indevido de licenças.

(ii) **Softwares proprietários:** quanto ao desenvolvimento de softwares proprietários, o ponto central é a proteção dos direitos de propriedade intelectual da organização sobre o software. Deste modo, é importante que os contratos celebrados com colaboradores ou terceiros envolvidos no desenvolvimento de software assegurem tais direitos, seja pela expressa menção aos direitos da organização sobre o software desenvolvido, seja pela indicação no contrato das atividades de desenvolvimento de software desenvolvidas pelo contratado, de modo a atender aos requisitos do artigo 4º da Lei de Software.

Além disso, são medidas recomendáveis:

- o registro no INPI de softwares proprietários, a depender da estratégia adotada para proteção de ativos intangíveis; e
- em caso de softwares proprietários utilizados comercialmente, assegurar-se de que os contratos de licenciamento de softwares proprietários a terceiros não coloquem em risco a titularidade dos direitos de propriedade intelectual da organização, especialmente quando há possibilidade de desenvolvimento de customizações.



Por fim, para o desenvolvimento de softwares proprietários é ainda importante possuir regras internas relacionadas ao uso de códigos-fonte *open source*, de modo a evitar o uso, em desenvolvimentos, de licenças *open source* que exijam, por exemplo, manutenção da mesma modalidade de licença em obras derivadas ou a disponibilização pública de código-fonte, incompatível com a exploração privada do programa de computador.

3 Segurança cibernética

Segurança cibernética refere-se às práticas e medidas adotadas para proteger os ativos de informação armazenados em ambiente digital – como em sistemas de computador, rede corporativa e dispositivos móveis – contra ameaças de acessos não autorizados, usos indevidos, divulgações ou alterações não autorizadas, destruição ou indisponibilidade.

No âmbito da Governança Digital, as medidas de segurança cibernética adotadas por uma organização de qualquer setor são essenciais para **garantir a integridade, confidencialidade e disponibilidade das informações e sistemas** e possuem alto valor estratégico, devendo estar alinhadas aos objetivos e boas práticas de governança gerais.

Nesse cenário, estratégias de contratação de tecnologia, transformação digital, ampliação de presença digital ou criação de novos produtos devem ser acompanhadas de **boas práticas e controles de segurança cibernética**, que não só visam **diminuir a exposição da organização a riscos**, como também **ampliam o grau de confiabilidade** da estratégia perante diversos *stakeholders*.

Além de diretrizes, princípios e obrigações diversas sobre segurança cibernética que podem ser extraídos da legislação brasileira, como a como a LGPD, o Marco Civil da Internet e seu decreto regulamentador (Decreto n. 8.771 de 11 de maio de 2016), diversos padrões não cogentes e técnicos são estabelecidos pelo mercado como práticas adequadas de segurança cibernética, como a norma ABNT NBR ISO/IEC 27001 e o NIST Cybersecurity Framework.

Além disso, também devem ser observadas as normas setoriais aplicáveis a cada organização, por exemplo, a **Resolução Normativa n. 964, de 14 de dezembro de 2021, da Agência Nacional de Energia Elétrica – ANEEL**, que versa sobre regras de segurança cibernética a serem adotadas pelos agentes do setor de energia elétrica, e a **Resolução BACEN CMN n. 4.893 de 26 de fevereiro de 2021**, que dispõe sobre política de segurança cibernética e requisitos de contratação de fornecedores de serviços em nuvem, que devem ser observados por instituições autorizadas a funcionar pelo Banco Central do Brasil.

Assim, partindo das normas aplicáveis ao negócio, da estratégia digital da organização e do grau de risco da atividade, pode-se estabelecer uma governança em segurança cibernética eficaz. Esta frente de governança pode englobar uma série de práticas, tais como:

- implementar **política de segurança cibernética** efetiva e compatível com a natureza e a estrutura da organização;
- estabelecer **controles de acesso** por meio de procedimentos administrativos e técnicos que garantam que apenas usuários autorizados tenham acesso a ativos de informação relevantes;
- **monitorar ameaças, gerir vulnerabilidades e riscos** por meio de rotinas preestabelecidas de identificação, avaliação e mitigação de vulnerabilidades nos sistemas de informação, bem como a implementação de medidas para reduzir o impacto de ameaças potenciais, incluindo, também, sistemas de monitoramento contínuo para detectar atividades suspeitas;
- estabelecer **regras de uso de equipamentos corporativos** para atividades profissionais.

Por fim, uma estratégia eficaz de Governança Digital e segurança cibernética inclui medidas de **resposta a incidentes de segurança** que possam comprometer a continuidade dos negócios e a confidencialidade, disponibilidade e integridade dos dados e ativos de informação da organização. Assim, é importante possuir um plano de resposta a incidentes, com diretrizes e procedimentos a serem observados por responsáveis previamente designados, desde a suspeita ou confirmação de ocorrência de um incidente até a completa resolução do caso.

Em síntese, a governança em segurança cibernética corresponde a um eixo central para a estabilidade e o desenvolvimento das organizações no contexto digital, além de ser crucial para assegurar a confiança das partes interessadas.

4 Ativos de Propriedade Intelectual

Para além de programas de computador, a gestão adequada dos direitos de propriedade intelectual, como marcas, nomes de domínio etc. – chamados de **ativos de PI** – também possui papel relevante e intersecção com a estruturação da Governança Digital de uma organização. Desse modo, a Governança Digital em propriedade intelectual envolve, entre outros aspectos, a adoção de estratégias de proteção adequadas de ativos de PI à transformação digital, bem como à presença online da organização, incluindo registros, ajustes contratuais e monitoramento de possíveis infrações.

Na prática, estas estratégias se traduzem em várias ações, exemplificadas a seguir:

- **Racionalização do portfólio de PI** como ponto de partida. É essencial identificar quais ativos são utilizados nas operações da organização, se estão adequadamente protegidos, sendo registrados e adequadamente controlados, inclusive para permitir a identificação de lacunas e de possíveis medidas corretivas.

- **Proteção dos ativos de PI** no contexto digital. Deve-se prestar atenção às brechas que podem não ser óbvias, mas são fundamentais para reduzir os riscos associados à crescente dependência de tecnologia e presença online. Dentro da Governança Digital, é importante enfatizar certas medidas específicas, como:

  - **registrar as marcas que diferenciam a organização**, seus serviços e produtos em todas as classes aplicáveis e formas utilizadas, especialmente **para proteger o uso em ambiente digital** (por exemplo, por meio da indicação de classe e especificação correta para serviço prestado em meio digital);

  - **assegurar que todos os nomes de domínio necessários para a operação estejam registrados**, incluindo domínios semelhantes ao principal ou que incorporam as marcas registradas da organização;

  - **implementar sistemas de monitoramento** para detectar e responder a violações de direitos de propriedade intelectual, como violações de marca registrada;

  - **negociar contratos envolvendo direitos autorais** relacionados a conteúdos criados internamente ou adquiridos de terceiros, com atenção para questões de titularidade, uso e distribuição do conteúdo;

  - assegurar que todos que manuseiem a propriedade intelectual da organização, incluindo funcionários e parceiros externos, estejam vinculados a **acordos de confidencialidade** para proteger informações confidenciais e/ou estratégicas;

- **implementar estratégia de proteção global dos ativos**, considerando que muitas organizações operam em múltiplas jurisdições, respeitando as particularidades locais.

5 Inteligência artificial

A inteligência artificial (**IA**) pode automatizar uma variedade de processos e tarefas relacionadas à Governança Digital, como análise de dados, detecção de anomalias de segurança, triagem de informações e tomada de decisões, aumentando a eficiência operacional e reduzindo custos. Ao mesmo tempo, a recente popularização da IA introduziu uma série de desafios jurídicos que devem ser cuidadosamente considerados no contexto da Governança Digital. Alguns dos principais desafios perpassam pelos seguintes questionamentos:

- **quem é responsável por decisões, danos ou erros decorrentes das ações da IA?**
- **como regulamentar o uso da IA para garantir sua utilização ética e segura, sem prejudicar a inovação?**
- **como garantir a transparência nos processos de tomada de decisão da IA e mitigar riscos relacionados aos algoritmos?**
- **como garantir que os resultados gerados pela IA (*outputs*) sejam precisos e confiáveis?**
- **como proteger a confidencialidade e direitos autorais?**
- **como garantir a segurança e legalidade dos dados utilizados e gerados pela IA?**

Essas são questões complexas cujas respostas têm sido objeto de debate em nível global. Iniciativas legislativas atuais, como o Projeto de Lei 2.338/2023, no Brasil, e o *EU AI Act*, aprovado na União Europeia, dentre outras em diversas jurisdições, buscam endereçar alguns dos desafios introduzidos pela IA.

Não obstante a inexistência de lei específica sobre o tema, é fundamental garantir que as práticas de IA adotadas estejam em conformidade com as leis gerais já vigentes e aplicáveis. Além disso, é possível resguardar-se, desde logo, das potenciais consequências negativas do uso da IA no presente – e de desdobramentos legais futuros – por meio de medidas de Governança em IA. Levando em conta as normas aplicáveis ao negócio, a estratégia digital da organização e o grau de risco da atividade, essas medidas podem incluir, por exemplo:

- avaliação de risco de IA, por meio da **avaliação de impacto algorítmico (AIA)**, para identificar e mitigar potenciais impactos negativos da IA sobre os indivíduos, organizações e sociedade como um todo;
- criação de um **comitê de ética em IA**, dedicado a orientar e monitorar práticas éticas relacionadas ao planejamento, desenvolvimento, implementação, uso e comercialização de IA;
- **políticas de uso de IA**, com diretrizes claras para o uso de sistemas de IA na organização;
- **políticas de desenvolvimento responsável de IA**, estabelecendo diretrizes para garantir que o desenvolvimento e a implementação de sistemas de IA, e tecnologias emergentes em geral, ocorram de forma ética, transparente, segura e responsável;
- revisão das **políticas de privacidade** para incluir tópicos sobre IA, quando aplicável, para abordar questões específicas relacionadas à IA e à proteção de dados, garantindo a devida transparência aos titulares de dados pessoais;
- medidas de **privacidade, ética e direitos humanos por design**[1], a fim de incorporar princípios e práticas relacionados à privacidade, ética e direitos humanos desde a concepção de produtos e serviços de IA.

[1] ***Privacy by Design*** é um conceito que estabelece parâmetros para incorporar a privacidade desde a fase inicial do design de sistemas, incluindo aqueles que utilizam inteligência artificial. Ele visa garantir que a privacidade dos usuários e dos dados de treinamento seja considerada e protegida desde a concepção do sistema.

Ethics by Design é uma abordagem metodológica que visa incorporar considerações éticas no design de sistemas, incluindo aqueles que usam IA. Ela assegura que os sistemas sejam projetados e utilizados de forma ética desde o seu início.

Human Rights by Design se concentra em garantir que as tecnologias, incluindo a IA, respeitem e promovam os direitos humanos. Isso implica considerar e proteger os direitos humanos desde o design inicial do sistema.

6 Aspectos Transacionais

A Governança Digital pode ter um impacto significativo nas estratégias de fusões e aquisições (M&A) de uma organização, tanto no que diz respeito à avaliação de alvos de M&A quanto em relação à integração de negócios pós-operação.

Sob a **ótica vendedora**, antecipar as discussões sobre potenciais fragilidades na Governança Digital que serão levantadas no curso da negociação permite uma maior celeridade nas negociações, bem como a captura de valor aos sócios/acionistas vendedores por meio de, por exemplo, **(i)** menor tempo para processamento da auditoria e, consequentemente, menos desvio de recursos do *core business*; **(ii)** evitar a sujeição do fechamento da operação a condições precedentes para regularização de pendências; e **(iii)** evitar descontos ou retenção de preço para fazer frente às contingências associadas às irregularidades de Governança Digital.

Sob a **ótica da compradora**, a identificação de tais fragilidades na Governança Digital de sociedades adquiridas garante a correta valorização dos ativos e a oportunidade de impor medidas saneadoras antes da conclusão da operação, quando ainda há alavanca negocial e a oportunidade de alinhar interesses pela via contratual.

Em **processos de auditoria** (*due diligence*) preliminares a operações societárias, é importante realizar uma avaliação abrangente dos ativos relevantes e procedimentos internos relacionados à Governança Digital da sociedade-alvo, a fim de identificar os riscos e oportunidades associados ao tema, incluindo avaliação dos ativos de propriedade intelectual, contratos de software relevantes para a infraestrutura tecnológica, práticas de segurança da informação e proteção de dados, dentre outros.

Da mesma forma, **após a conclusão da operação**, a Governança Digital desempenha um papel fundamental para a integração bem-sucedida da sociedade-alvo com a compradora, podendo incluir, por exemplo, estratégias para aplicação ou harmonização de políticas e procedimentos de segurança cibernética, consolidação e migração de sistemas de tecnologia da informação, implementação de melhores práticas de governança de dados e conformidade com a legislação aplicável, entre outras. Uma Governança Digital eficaz durante o processo de integração contribui, ainda, para a fluida continuidade dos negócios digitais e minimização de riscos operacionais.

Como exemplos de itens de Governança Digital comumente discutidos em operações de M&A, destacam-se:

Na preparação da operação:

- revisar os contratos de trabalho de prestação de serviços e de administração para garantir que os **colaboradores reconheçam a transferência de titularidade** dos frutos dos trabalhos desenvolvidos para a sociedade contratante;
- **transferir para a sociedade a titularidade de nomes de domínio, marcas e outros direitos de propriedade intelectual** sujeitos a registro (dado que é comum que os sócios registrem parte de tais ativos em nome próprio ou de pessoas afiliadas);
- revisar a **adequação das práticas** de tratamento de dados e informações estratégicas;
- garantir que as práticas e **procedimentos de Governança Digital estejam propriamente documentados**, de forma a possibilitar a sua apresentação a potenciais interessados.

Na fase de negociação da operação:

- garantir que a troca de informações seja suportada por **acordos de confidencialidade** robustos e por meios seguros;
- certificar que a troca de **informações comercialmente sensíveis** (tais como dados de formação de preço, custo de produção, informações financeiras individualizadas, dados de mercado) seja revisada por um advogado especializado em lei antitruste, de forma a evitar a imposição de penalidades;
- discutir o **faseamento da disponibilização de informações** conforme a assertividade do interesse das partes na negociação;
- discutir uma agenda e critérios objetivos de **como a operação será apresentada** ao mercado, colaboradores, clientes, fornecedores e demais *stakeholders*.

Na fase após a conclusão da operação:

- discutir uma agenda para a **transição, compatibilização e harmonização de práticas** e procedimentos de Governança Digital;
- criar controles com **metas e protocolos objetivos** para a implementação das medidas de saneamento de pendências que não tenham sido endereçadas nos contratos.

7 Aspectos Tributários

No contexto de digitalização da economia, surgem desafios relacionados à tributação aplicável aos modelos de negócio digitais. O sistema tributário brasileiro foi construído sobre uma premissa de segregação das atividades econômicas entre fornecimento de **bens x prestação de serviços**, e muitos dos modelos de negócio digitais não se conformam a esta dicotomia.

Durante muitos anos discutiu-se sobre a tributação aplicável a operações com **software**. Ainda com base na dicotomia entre bens x serviços, o Supremo Tribunal Federal ("STF") adotou no julgamento do RE 176.626-3, em 1988, separação entre software sob encomenda – cujo desenvolvimento e licenciamento eram considerados como prestação de serviços, sujeita ao Imposto sobre Serviços de Qualquer Natureza ("ISS") – e software não exclusivo, ou "de prateleira" – considerado como mercadoria cuja circulação estaria sujeita ao Imposto sobre a Circulação de Mercadorias e Serviços ("ICMS").

Entretanto, com o desenvolvimento do mercado e a introdução de novas modalidades de software acessíveis via download e via nuvem (*Software as a Service* ou SaaS), esta separação entre software sob encomenda e software de prateleira deixou de ser suficiente para regular o conflito de competência entre ISS e ICMS, e foi então revista pelo STF, que passou a reconhecer que todas as transações envolvendo licenças de uso de software estariam sujeitas ao ISS, independentemente de se tratar de software por encomenda ou de prateleira[2]. Embora não tenha sido o escopo da discussão, a mudança de posicionamento do STF sobre a qualificação das operações envolvendo licenças de uso de software tem reverberado também na seara federal, com a revisão de alguns entendimentos da Receita Federal do Brasil sobre os regimes aplicáveis e tributos incidentes sobre essas operações.

[2] Conforme decisão proferida no julgamento conjunto das Ações Diretas de Inconstitucionalidade ("ADI") nº 1945 e 5659, em 24.02.2021, alterando seu posicionamento anterior.

Considerar essas discussões na estratégia de Governança Digital de uma organização é importante porque geram reflexos, por exemplo, na definição do percentual de presunção aplicável à receita bruta decorrente de tais operações, auferida por pessoas jurídicas sujeitas à tributação pelo Imposto de Renda da Pessoa Jurídica ("IRPJ") e pela Contribuição Social sobre o Lucro Líquido ("CSLL") segundo o regime do lucro presumido, e nos tributos incidentes sobre as remessas ao exterior para remuneração por licença de uso e licença de distribuição de software – e.g., PIS/Cofins-Importação; Contribuição para a Intervenção no Domínio Econômico ("CIDE"); Imposto de Renda Retido na Fonte ("IRRF") etc.

Outro exemplo de complexidades tributárias decorrentes da digitalização da economia e da migração de diversas atividades para o ambiente virtual é a **omnicanalidade** (*omninchannel*). A omnicanalidade corresponde à integração dos diferentes canais de venda e atendimento ao cliente (i.e., loja física, site, app, rede social etc.). A despeito das muitas vantagens que a omnicanalidade pode trazer para varejistas e clientes, a conformação deste modelo de negócios às regras tributárias atuais é desafiadora, uma vez que parte da premissa de uma atuação conjunta de diferentes pessoas jurídicas que ofertam suas soluções em benefício de uma única operação de venda, mas que, via de regra, devem apurar seus resultados e tributar suas operações em bases individuais – o que implica discussões que reverberam na apuração de IRPJ/CSLL, PIS/Cofins, ISS e ICMS. Neste contexto, é importante que os aspectos fiscais da omnicanalidade sejam ponderados e refletidos nas estruturas contratuais.

Por fim, temos no horizonte a implementação da **Reforma Tributária**, introduzida pela Emenda à Constituição nº 132/2023, que altera substancialmente a atual forma de tributação sobre o consumo, substituindo diversos tributos "indiretos" (ICMS, ISS, Imposto sobre Produtos Industrializados – "IPI", Contribuição ao Programa de Integração Social – "PIS" e Contribuição para o Financiamento da Seguridade Social – "Cofins") por basicamente três novos tributos: o Imposto sobre Bens e Serviços ("IBS") e a Contribuição sobre Bens e Serviços ("CBS"), que incidirão sobre operações com bens materiais ou imateriais, inclusive direitos, ou com serviços e importação não habitual; e o Imposto Seletivo ("IS").

A Reforma Tributária está sujeita a um período de transição, que será iniciado em 2026 e irá até 2033, a partir de quando o novo modelo substituirá completamente o anterior.

Ainda há diversos pontos a serem definidos (e.g. alíquota, mecânica de apuração e recolhimento) e os projetos de leis complementares que irão regular a Reforma Tributária estão em discussão na Câmara dos Deputados – que poderão impactar a estratégia de Governança Digital das organizações no futuro.

A expectativa é de que haverá uma simplificação geral no sistema de tributação sobre o consumo, mas com reflexos importantes no setor de tecnologia e economia digital. Particularmente em razão de um potencial aumento da carga tributária do setor e medidas que impõem responsabilidade para plataformas digitais (e.g. marketplaces) em relação ao recolhimento dos tributos nas operações realizadas sob seu intermédio.

8 Aspectos Trabalhistas

Se as transformações digitais implicam a necessidade do desenvolvimento de um modelo de Governança Digital bem definido, à medida em que as novas tecnologias assumem, de forma cada vez mais intensa, grande protagonismo na atual sociedade, as relações de trabalho também são grandemente influenciadas pelas mudanças em questão.

Não por acaso, em 2017, quando foi promulgada a Lei 13.467, que ficou conhecida como a "Reforma Trabalhista", sobrevieram as primeiras disposições legais a respeito do modelo de Teletrabalho.

O Teletrabalho veio à tona em um cenário de importantes mudanças conjunturais, em que as empresas passaram a implementar modelos diferenciados de prestação de serviços, sem que houvesse a necessidade de o empregado estar, fisicamente e todos os dias, nas dependências da empresa. A necessidade de regulamentação, aliás, acabaria por ser reforçada com o advento da pandemia, ocasionada pela COVID-19.

Neste contexto, a legislação estabelece requisitos para o regular exercício do Teletrabalho pelos empregados. Há necessidade de que haja **cláusula específica no Contrato de Trabalho** – ou em eventual aditivo – quanto à prestação de serviços no modelo de Teletrabalho. O mesmo contrato ou aditivo deverá, ainda, tratar a respeito da **responsabilidade pela aquisição e manutenção dos equipamentos e infraestrutura**.

Ainda, sempre que possível, recomenda-se que haja a **estruturação de política interna voltada especificamente para dispor sobre o Teletrabalho e todas as suas nuances**, na qual devem ser abordadas as regras referentes ao regime e, adicionalmente, as definições de segurança quanto a dados, informações confidenciais, destruição e conservação de documentos etc.

Vale notar que, em 2022, houve atualização do regramento atinente ao Teletrabalho, ocasião em que passou a ser expressa a possibilidade de o modelo ser implementado por jornada ou tarefa, o que interfere no controle de jornada dos teletrabalhadores; tratou-se sobre a utilização dos equipamentos do empregador fora da jornada de trabalho; da aplicação da legislação brasileira aos empregados que trabalham remotamente fora do Brasil, além de outras ponderações que dão novos contornos ao modelo, assim como trazem novas exigências.

Outros pontos que chamam a atenção quando se pensa na Governança Digital inserida em meio às relações de trabalho são:

(i) a **responsabilidade e o limite de fiscalização, pelo empregador**, quanto aos dados pessoais de seus próprios empregados ou de todas as demais partes relacionadas na cadeia de valor (prestadores de serviços, consumidores, fornecedores etc.), em uma vertente que possui forte relação com a LGPD, e

(ii) a responsabilização dos empregados em situações nas quais estes falham com o dever de preservar os dados de partes relacionadas com o empregador, tais como os clientes[3], o que reforça a importância de **normas muito bem estruturadas a fim de identificar claramente os potenciais ilícitos, quando se trata de lidar com fluxos digitais de dados**.

Assim, a preservação das informações, sejam estas pessoais dos empregados, sejam as pertencentes à empresa e tidas como confidenciais, torna-se foco de atenção no âmbito da Governança Digital, atraindo para a realidade empresarial as discussões relativas às hipóteses de tratamento de dados e de respectivas violações.

O respeito à legislação trabalhista, em meio a discussões tão contemporâneas, é também importante para a construção de um ambiente seguro, em consonância com um sistema de Governança Digital robusto.

[3] Como ocorrido na decisão proferida pelo Tribunal Regional do Trabalho de São Paulo no processo nº 1000612-09.2020.5.02.0043.

9 Educação e aculturamento

Por fim, quando se trata de Governança Digital, é importante ressaltar que as pessoas desempenham um papel fundamental na prevenção dos riscos associados em cada frente abordada neste material.

Colaboradores bem treinados são, no limite, a primeira linha de defesa contra os riscos relacionados à atuação digital da organização, na medida em que são capazes, por exemplo, de identificar e responder proativamente a possíveis ameaças cibernéticas, como *phishing* e *malwares*, bem como de agir de forma íntegra frente a dilemas éticos e regulatórios relacionados à inovação.

Assim, **a promoção de ações de educação e aculturamento é parte essencial de uma Governança Digital efetiva**. Estas iniciativas não apenas protegem as organizações de possíveis ameaças, mas também promovem a cultura de segurança e conformidade em todos os seus níveis, garantindo uma operação digital mais segura e sustentável.

Medidas de **educação**, em linhas gerais, visam a ampliação do **conhecimento teórico** e **ensinamento de boas práticas** em questões relacionadas à Governança Digital, podendo incluir **programas de treinamento, workshops, seminários e materiais educacionais** para os colaboradores.

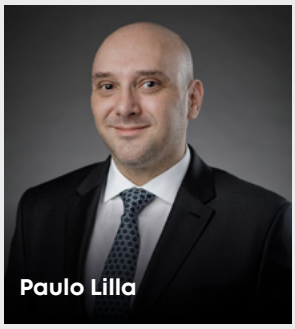
Já as ações de **aculturamento** visam promover uma cultura organizacional que valoriza a Governança Digital e reconheça sua importância para o sucesso da organização. Perpassam, por exemplo, pela criação de **políticas internas** que incentivem comportamentos responsáveis em relação ao tema, bem como pelo desenvolvimento de **programas de incentivo e valorização de comportamentos alinhados à cultura visada** e promoção de **eventos e atividades de engajamento**.

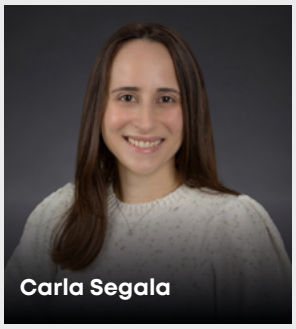
Essas medidas também podem ser estendidas a terceiros, como fornecedores e parceiros de negócio, conforme aplicável, na medida em que uma cadeia de fornecimento e um ecossistema digital seguro dependem da conscientização e da colaboração de todos os envolvidos.

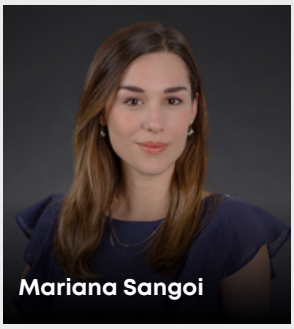
Nossa atuação

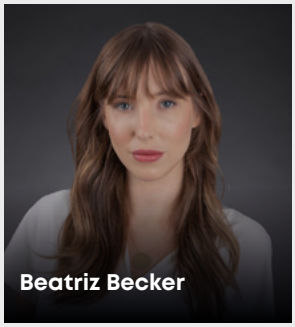
Temos uma equipe especializada em **Tecnologia, Proteção de Dados e Propriedade Intelectual**, bem como **equipe multidisciplinar focada no setor de tecnologia**, composta por diversas práticas do escritório, para atender os nossos clientes em questões relacionadas à Governança Digital e outras demandas pertinentes.

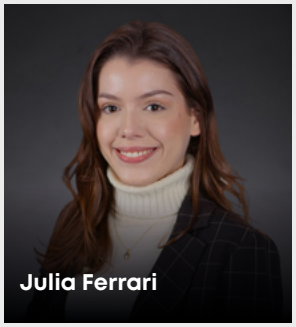
Prática de Tecnologia, Proteção de Dados e Propriedade Intelectual



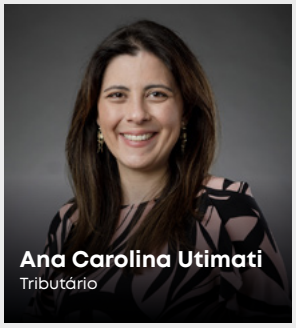


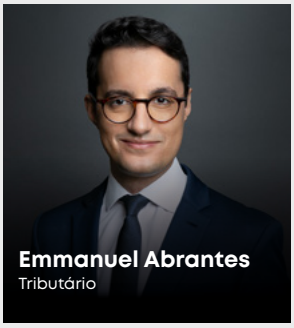




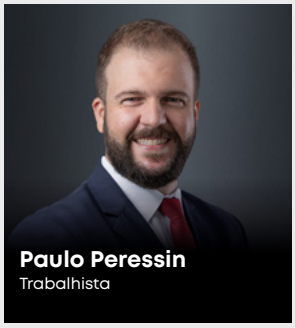


Sócios do Grupo Multidisciplinar em Tecnologia





Sócio Colaborador



Lefosse

São Paulo
Rua Tabapuã, 1227 - 14º andar
04533-014 Itaim Bibi
São Paulo SP Brasil
+ 55 11 3024-6100

Rio de Janeiro
Praia do Flamengo, 200 – 20º andar
22210-901 Flamengo
Rio de Janeiro RJ Brasil
+ 55 21 3263-5480

Brasília
SCS Quadra 09, Edifício Parque Cidade Corporate
Torre B, 8º andar
70308-200 Asa Sul
Brasília DF Brasil
+ 55 61 3957-1000

lefosse.com

Siga-nos nas
redes sociais