Por Thomas Hannickel, Compliance Officer e DPO da Legitimuz, especialista em Direito Digital e Regulação

Existe um equívoco recorrente na forma como muitas empresas tratam o compliance digital. À medida que novas normas passaram a regular a economia digital, consolidou-se a percepção de que bastaria adequar processos à legislação mais recente. Primeiro veio o Marco Civil da Internet, depois a Lei Geral de Proteção de Dados (LGPD) e, agora, o ECA Digital. Como se cada nova regra substituísse a anterior.

Não foi isso que aconteceu.

O Brasil passou a construir um sistema regulatório em que essas normas coexistem e incidem sobre uma mesma operação digital. Marco Civil, LGPD e ECA Digital regulam aspectos distintos das

relações digitais e, justamente por isso, devem ser interpretados de forma complementar.

Essa diferença produz impactos que vão além do jurídico.

Um único fluxo digital pode envolver autenticação biométrica, tratamento de dados pessoais, prevenção à fraude, verificação de idade e gestão de riscos. Para o usuário, trata-se de uma única experiência. Para a empresa, porém, essa mesma jornada reúne diferentes obrigações legais que precisam ser atendidas simultaneamente.

É justamente nesse ponto que muitas organizações ainda enfrentam dificuldades.

Nos últimos anos, a LGPD passou a ocupar posição central nos programas de governança. Isso contribuiu para amadurecer a discussão sobre proteção de dados, mas também criou a impressão de que a conformidade digital poderia ser resumida à privacidade.

Hoje, essa visão já não é suficiente.

O Marco Civil disciplina aspectos relacionados ao funcionamento das relações digitais, como a guarda de registros e a responsabilidade dos provedores. A LGPD estabelece regras para o tratamento de dados pessoais. O ECA Digital acrescenta uma nova camada de proteção ao exigir mecanismos específicos voltados à segurança de crianças e adolescentes no ambiente digital, incluindo formas confiáveis de verificação de idade.

Embora tratem da mesma economia digital, essas normas respondem a perguntas diferentes.

O Marco Civil disciplina como a relação digital acontece. A LGPD regula como os dados pessoais são tratados. O ECA Digital estabelece quais cuidados adicionais devem existir quando essa operação envolve crianças e adolescentes.

O problema é que as empresas continuam organizando seus programas de conformidade da mesma forma que organizam suas estruturas internas: jurídico de um lado, tecnologia de outro, produto, segurança da informação e privacidade em frentes distintas.

O regulador, entretanto, não analisa departamentos.

Ele analisa operações.

Essa diferença altera a própria lógica do compliance digital. Já não basta demonstrar conformidade com uma legislação específica. É necessário evidenciar que uma mesma operação foi estruturada para atender, simultaneamente, às diferentes exigências regulatórias que incidem sobre ela.

Talvez nenhum exemplo represente melhor essa transformação do que o onboarding digital.

Aquilo que antes era apenas uma etapa de cadastro passou a concentrar algumas das decisões mais sensíveis de toda a operação. É nesse momento que identidades são verificadas, documentos e dados biométricos são tratados, sinais de fraude são analisados e, em determinados serviços, mecanismos de verificação de idade precisam ser aplicados.

Há apenas uma jornada para o usuário.

Mas, do ponto de vista regulatório, diferentes camadas de responsabilidade coexistem sobre essa mesma experiência.

Essa constatação muda a forma como o próprio conceito de compliance deve ser compreendido.

Durante muito tempo, conformidade significava verificar se determinada obrigação legal havia sido cumprida. Hoje, essa lógica já não basta. A expectativa regulatória é que as empresas demonstrem

que seus processos foram concebidos para atender diferentes exigências legais de forma integrada, sem comprometer segurança, privacidade ou experiência do usuário.

Isso desloca parte importante da discussão para as áreas de tecnologia e produto.

A forma como uma identidade é validada, os critérios de autenticação adotados, o momento em que determinados dados são coletados e os mecanismos utilizados para proteger públicos vulneráveis deixam de ser decisões exclusivamente técnicas. Passam a integrar a estratégia de governança da organização.

O ECA Digital evidencia essa transformação.

Ao exigir mecanismos confiáveis de verificação de idade e afastar soluções baseadas apenas na autodeclaração, a legislação não cria apenas uma nova obrigação jurídica. Ela influencia diretamente a forma como as plataformas estruturam suas jornadas digitais e administram riscos.

Esse movimento revela uma mudança importante na evolução regulatória.

As primeiras gerações de normas buscavam disciplinar o comportamento das empresas. As mais recentes passaram a influenciar o próprio desenho das operações digitais.

Nesse cenário, discutir compliance apenas sob a perspectiva jurídica tornou-se insuficiente. A conformidade passa a depender da capacidade de integrar Direito, tecnologia, produto, segurança da informação, privacidade e prevenção à fraude em torno de uma mesma estratégia.

É justamente dessa convergência que surge um conceito que tende a ganhar cada vez mais relevância: a governança da confiança digital.

Ela parte de uma premissa simples. Identidade, proteção de dados, prevenção à fraude e segurança da informação deixaram de ser agendas independentes. Quando tratadas de forma integrada, fortalecem não apenas a conformidade regulatória, mas também a resiliência e a credibilidade da operação.

Essa mudança ajuda a explicar por que tecnologias de identidade digital assumiram um papel estratégico.

Durante muito tempo, mecanismos de verificação de identidade eram vistos apenas como ferramentas para cadastro ou cumprimento de requisitos de *Know Your Customer* (KYC). Hoje, desempenham uma função muito mais ampla: sustentam políticas de prevenção à fraude, apoiam processos de verificação de idade, fortalecem programas de proteção de dados e contribuem para a produção de evidências de conformidade perante diferentes autoridades.

Naturalmente, tecnologia não substitui governança.

Nenhuma solução tecnológica é capaz de compensar a ausência de processos consistentes ou de decisões corporativas responsáveis. Da mesma forma, nenhuma legislação, isoladamente, é capaz de produzir confiança.

A confiança resulta da combinação entre regras claras, tecnologia adequada e governança consistente.

Por isso, maturidade regulatória já não pode ser medida apenas pela existência de políticas internas ou controles formais. O verdadeiro diferencial está na capacidade de transformar requisitos legais em operações coerentes, capazes de equilibrar proteção, eficiência e experiência do usuário.

A evolução da regulação digital brasileira demonstra que a principal mudança não está apenas no

surgimento de novas obrigações legais, mas na forma como elas passam a influenciar a construção das operações digitais.

Durante muito tempo, a pergunta que orientava os programas de compliance era relativamente simples: a empresa está adequada à legislação? Hoje, essa pergunta evoluiu. O desafio passa a ser compreender se a operação foi concebida para responder, de forma integrada, às diferentes responsabilidades que recaem sobre ela.

Essa mudança representa um novo estágio da maturidade regulatória.

O Marco Civil da Internet estruturou as bases das relações digitais. A LGPD consolidou regras para o tratamento de dados pessoais e fortaleceu a cultura de prestação de contas. O ECA Digital amplia esse sistema ao incorporar deveres específicos de proteção para crianças e adolescentes, exigindo que segurança e responsabilidade façam parte do próprio desenho das plataformas.

Nenhuma dessas normas substitui a anterior. Ao contrário, elas se complementam e ampliam o conjunto de responsabilidades das organizações.

Por isso, o maior desafio já não é conhecer cada legislação individualmente, mas compreender como elas se conectam dentro de uma mesma operação.

Essa é uma discussão que extrapola o departamento jurídico. Ela envolve tecnologia, produto, segurança da informação, privacidade, prevenção à fraude e liderança executiva. Todas essas áreas passaram a compartilhar a responsabilidade de construir operações capazes de conciliar inovação, experiência do usuário e conformidade regulatória.

Essa convergência tende a se intensificar nos próximos anos. O avanço das discussões sobre inteligência artificial, identidade digital, autenticação eletrônica e responsabilidade das plataformas aponta para um cenário em que a capacidade de adaptar operações a diferentes exigências regulatórias será um diferencial competitivo.

Nesse contexto, a confiança deixa de ser apenas um atributo de marca. Ela passa a ser resultado de uma governança consistente, construída pela integração entre processos, tecnologia e gestão de riscos.

É justamente essa integração que define o que chamo de governança da confiança digital: uma abordagem em que identidade, proteção de dados, prevenção à fraude e segurança da informação deixam de atuar como disciplinas isoladas para compor uma única estratégia de proteção das relações digitais.

No fim, talvez essa seja a principal lição da evolução regulatória brasileira. O desafio das empresas já não é apenas acompanhar novas leis, mas desenvolver operações preparadas para responder a um ambiente regulatório cada vez mais integrado. Organizações que compreenderem esse movimento estarão mais aptas a transformar conformidade em confiança — e confiança em um ativo estratégico para seus negócios.

Sobre Thomas Hannickel

Thomas Hannickel é Compliance Officer e Data Protection Officer (DPO) da Legitimuz. Especialista em Direito Digital, proteção de dados e regulação, atua na interseção entre tecnologia, privacidade e conformidade regulatória, com foco em identidade digital, KYC, AML e biometria. Professor na FACAMP, alia a atuação acadêmica à experiência prática na estruturação de programas de governança para operações digitais altamente reguladas. Na Legitimuz, lidera as iniciativas relacionadas à privacidade, proteção de dados e conformidade regulatória, além de representar a empresa em discussões junto à ANPD, incluindo a elaboração de subsídios técnicos sobre verificação biométrica apresentados à consulta pública da Autoridade em 2026.

Fonte: Deepr, em 22.07.2026