

PROPOSTA DE LEI DE PROTECÇÃO DE DADOS PESSOAIS EM MOÇAMBIQUE: O QUE ESTÁ EM CAUSA?

PROPOSED PERSONAL DATA PROTECTION LAW IN MOZAMBIQUE: WHAT IS AT STAKE?

POLICY BRIEF

1. Introdução

Se aplicada devidamente, a Proposta de Lei de Protecção de Dados Pessoais pode representar um passo estrutural para a consolidação do Estado de Direito digital em Moçambique. A proposta actualmente na Assembleia da República procura preencher uma lacuna normativa relevante: transformar a protecção de dados pessoais de uma garantia constitucional e sectorial dispersa num regime jurídico próprio, aplicável ao tratamento físico e digital por entidades públicas e privadas¹.

A referida proposta tem uma arquitectura ambiciosa, dado que define princípios, bases de licitude, categorias especiais de tratamento, direitos dos titulares, poderes da autoridade reguladora, regras de transferências internacionais, deveres de segurança, notificação de incidentes, avaliação de impacto, sanções e mecanismos de tutela. A sua qualidade final dependerá, contudo, de três factores: independência regulatória real, clareza das excepções em matéria de segurança e interesse público, e capacidade administrativa para tornar a conformidade viável no sector público, nas empresas e nas organizações da sociedade civil.²

É procurando olhar para os elementos de mérito e desafios que o presente policy brief aborda, de forma crítica, os elementos referentes ao respeito do quadro geral de usufruto de direitos digitais em Moçambique, bem como dos direitos fundamentais.

1. Introduction

If properly implemented, the Personal Data Protection Bill could represent a structural step towards consolidating the digital rule of law in Mozambique. The proposal currently before the Assembly of the Republic seeks to fill a significant regulatory gap: transforming personal data protection from a dispersed constitutional and sectoral guarantee into a dedicated legal regime applicable to physical and digital processing by public and private entities.

The proposal has an ambitious architecture, as it defines principles, lawful bases, special categories of processing, data subject rights, powers of the regulatory authority, rules on international transfers, security duties, incident notification, impact assessment, sanctions and redress mechanisms. Its final quality will, however, depend on three factors: real regulatory independence, clarity of exceptions relating to security and public interest, and administrative capacity to make compliance viable in the public sector, in companies and in civil society organizations.

Seeking to examine both its merits and its challenges, this policy brief critically addresses the elements relating to respect for the general framework for the enjoyment of digital rights in Mozambique, as well as fundamental rights.

2. O mérito da proposta

É de entendimento quase unânime que a Proposta de Lei de Protecção de Dados Pessoais representa um avanço relevante para o reforço do quadro jurídico moçambicano em matéria de

privacidade e protecção de dados. Ao estabelecer um regime geral aplicável ao tratamento de dados pessoais por entidades públicas e privadas, o instrumento protege uma garantia constitu-

2. The merits of the proposal

It is almost unanimously understood that the Personal Data Protection Bill represents an important step forward in strengthening Mozambique's legal framework on privacy and data

protection. By establishing a general regime applicable to the processing of personal data by public and private entities, the instrument protects a long-pending constitutional guarantee and

1. Cf. Fundamentação da Proposta; artigos 1 e 2 da Proposta de Lei de Protecção de Dados Pessoais.

2. Cf. artigos 5, 11, 12, 13, 24 a 30, 36 a 38, 43, 46, 48 e 51.

“ Destaca-se a consolidação de uma abordagem assente nos direitos fundamentais ”

cional há muito pendente e aproxima o país aos padrões internacionais nesta matéria.³

Entre os seus principais méritos destaca-se a consolidação de uma abordagem assente nos direitos fundamentais, conferindo expressão normativa a princípios como a privacidade, a autodeterminação informativa, a transparência, a não discriminação e os direitos de acesso, rectificação, eliminação e portabilidade dos dados pessoais. Paralelamente, a proposta adopta uma matriz moderna de licitude do tratamento, reconhecendo diferentes fundamentos jurídicos para o tratamento de dados, para além do consentimento, em consonância com as tendências internacionais.⁴

A proposta de lei merece igualmente destaque por reconhecer que determinadas operações de tratamento de dados pessoais acarretam riscos acrescidos para os direitos dos cidadãos, estabelecendo regras

específicas para categorias especiais de dados, nomeadamente: dados de crianças, vídeo-vigilância, gravação de chamadas, crédito e solvabilidade, bem como para o tratamento realizado por entidades públicas. Introduce, ainda, importantes mecanismos de responsabilização organizacional, incluindo a designação de encarregados de protecção de dados, registos de tratamento, avaliações de impacto, medidas de segurança, programas de boas práticas e um regime sancionatório aplicável ao incumprimento das obrigações legais.

No seu conjunto, estas disposições aproximam Moçambique das boas práticas internacionais em matéria de protecção de dados pessoais e criam condições mais favoráveis para o reforço da confiança nos serviços digitais, na administração pública electrónica, na economia digital e nas transferências internacionais de dados. Não obstante estes avanços, alguns aspectos da proposta de lei poderão beneficiar de aperfeiçoamentos durante o processo legislativo, tal como abaixo se propõe.

“ Among its main merits is the consolidation of an approach grounded in fundamental rights ”

brings the country closer to international standards in this area.

Among its main merits is the consolidation of an approach grounded in fundamental rights, giving normative expression to principles such as privacy, informational self-determination, transparency, non-discrimination, and the rights of access, rectification, erasure and portability of personal data. At the same time, the proposal adopts a modern framework for the lawfulness of processing, recognizing different legal grounds for data processing beyond consent, in line with international trends.

The bill also deserves recognition for acknowledging that certain personal data processing operations pose heightened risks to citizens' rights, establishing specific rules for special categories of data,

namely: children's data, video surveillance, call recording, credit and solvency data, as well as processing carried out by public entities. It also introduces important organizational accountability mechanisms, including the designation of data protection officers, processing records, impact assessments, security measures, good practice programs and a sanctions regime applicable to non-compliance with legal obligations.

Taken together, these provisions bring Mozambique closer to international good practice on personal data protection and create more favorable conditions for strengthening trust in digital services, electronic public administration, the digital economy and international data transfers. Notwithstanding these advances, some aspects of the bill could benefit from improvement during the legislative process, as proposed below.

3. Governação e independência regulatória

A proposta propõe um Sistema Nacional de Protecção de Dados Pessoais, composto por um Conselho Nacional de coordenação político-estratégica e por uma Autoridade Nacional de Protecção de Dados. O Conselho deverá ser presidido pelo Primeiro-Ministro e inclui sectores de defesa, segurança, TIC, justiça, finanças, saúde,

educação, reguladores, Ministério Público, SERNIC, CSIRT, sector empresarial, academia e sociedade civil.⁵

A coordenação multisectorial é meritosa, porque a protecção de dados atravessa políticas públicas, segurança, economia digital e direitos fundamentais. O risco está em permitir que a

3. Governance and regulatory independence

The proposal provides for a National Personal Data Protection System, composed of a National Council for political and strategic coordination and a National Data Protection Authority. The Council should be chaired by the Prime Minister and includes the defense, security, ICT, justice, finance,

health and education sectors, regulators, the Public Prosecutor's Office, SERNIC, CSIRT, the business sector, academia and civil society.

Multisectoral coordination is meritorious, because data protection cuts across public policy, security, the digital

3. Cf. Fundamentação da Proposta de Lei; artigos 1.º, 2.º, 4.º e 5.º da Proposta de Lei de Protecção de Dados Pessoais.

4 Cf. artigos 5.º, 13.º, 24.º a 30.º da Proposta de Lei.

5 Cf. artigos 15.º a 21.º, 31.º a 46.º e 51.º a 55.º da Proposta de Lei.

6 Cf. artigos 6, 7, 8 e 9.

“O risco está em permitir que a coordenação política se confunda com supervisão independente.”

coordenação política se confunda com supervisão independente. Por isso, o texto deve delimitar com maior rigor que o Conselho define orientações estratégicas e acompanha políticas públicas, mas não interfere na fiscalização, decisões sancionatórias, autorizações de transferências, tratamento de queixas ou pareceres técnicos da ANPD.⁷

O outro aspecto relevante prende-se com a opção de atribuir as funções de Autoridade Nacional de Protecção de Dados (ANPD) à Entidade Reguladora de Tecnologias de Informação e Comunicação. Embora o artigo 11 consagre a independência funcional e a imparcialidade da Autoridade, a proposta não explicita o racional desta opção institucional, nem esclarece de que forma uma entidade reguladora sectorial exercerá competências directamente relacionadas com a protecção de um direito fundamental. Atribuir estas funções a uma entidade já existente pode constituir uma

solução eficiente do ponto de vista administrativo e financeiro. Contudo, esta escolha suscita questões quanto ao modelo institucional adoptado, sobretudo porque a proposta não clarifica se a protecção de dados será exercida como uma função autónoma, dotada de organização e capacidade próprias, ou como uma competência integrada na estrutura regulatória já existente. Esta indefinição assume especial importância num contexto em que a Autoridade será chamada a fiscalizar simultaneamente operadores económicos, entidades públicas e órgãos do próprio Estado. Tratando-se de uma opção estruturante para o Sistema Nacional de Protecção de Dados, seria desejável que a própria lei definisse, com maior precisão, o estatuto institucional da ANPD e os mecanismos que asseguram a sua autonomia no exercício das suas competências, permitindo à Assembleia da República pronunciar-se sobre elementos centrais da arquitectura institucional da futura Autoridade, em vez de remeter essas opções para regulamentação posterior.⁸

economy and fundamental rights. The risk lies in allowing political coordination to be confused with independent supervision. For that reason, the text should define more rigorously that the Council sets strategic guidelines and monitors public policies, but does not interfere in oversight, sanctioning decisions, transfer authorizations, complaint handling or technical opinions issued by the ANPD.

Another relevant aspect concerns the decision to assign the functions of the National Data Protection Authority (ANPD) to the Information and Communication Technologies Regulatory Entity. Although article 11 enshrines the Authority's functional independence and impartiality, the proposal does not explain the rationale for this institutional choice, nor does it clarify how a sectoral regulator will exercise powers directly related to the protection of a fundamental right. Assigning these functions to an existing entity may be an efficient solution from an administrative and financial point of view; however, this choice raises questions about the institutional model adopted,

“The risk lies in allowing political coordination to be confused with independent supervision.”

especially because the proposal does not clarify whether data protection will be exercised as an autonomous function, endowed with its own organization and capacity, or as a competence integrated into the existing regulatory structure. This ambiguity is particularly important in a context in which the Authority will be called upon to supervise, at the same time, economic operators, public entities and State bodies themselves. Since this is a structural choice for the National Data Protection System, it would be desirable for the law itself to define, with greater precision, the institutional status of the ANPD and the mechanisms that ensure its autonomy in the exercise of its powers, allowing the Assembly of the Republic to pronounce itself on central elements of the future Authority's institutional architecture instead of referring these choices to subsequent regulation.

4. Protecção dos direitos fundamentais

A proposta confere eficácia prática ao direito à privacidade, permitindo que os titulares exerçam um controlo efectivo sobre a recolha, utilização, conservação e circulação dos seus dados pessoais, não se reduzindo a protecção da privacidade a uma mera questão de declaração de princípios.⁹

O instrumento já em sede do parlamento também acerta ao impor padrões reforçados para dados sensíveis, crianças, dados de saúde, dados biométricos,

dados de condenações penais, video-vigilância, gravação de chamadas e tratamento de dados por autoridades públicas. Estes domínios concentram riscos de vigilância indevida, discriminação, exclusão social, abuso económico e exposição de pessoas vulneráveis.¹⁰

Ainda assim, a eficácia dos direitos dependerá da precisão das excepções. O artigo 25 admite limitações ao direito de acesso por segurança do

4. Protection of fundamental rights

The proposal gives practical effect to the right to privacy, allowing data subjects to exercise effective control over the collection, use, retention and circulation of their personal data, so that privacy protection is not reduced to a mere statement of principles.

The instrument already before Parliament is also right to impose enhanced standards for sensitive data, children's data, health data, biometric data, data on criminal convictions, video surveillance, call

recording and data processing by public authorities. These domains concentrate risks of undue surveillance, discrimination, social exclusion, economic abuse and exposure of vulnerable people.

Even so, the effectiveness of rights will depend on the precision of the exceptions. Article 25 allows limitations on the right of access on grounds of State security, criminal investigation, judicial secrecy and scientific research. These restrictions should be interpreted as necessary, proportiona-

6 Cf. artigos 6, 7, 8 e 9.

7 Cf. artigos 9, 11 e 12.

8 Cf. artigos 10 e 11.

9 Cf. artigos 10 e 11.

10 Cf. artigos 15, 17, 18, 20, 21, 31, 32 e 33.

Estado, investigação criminal, segredo de justiça e investigação científica. Essas restrições devem ser interpretadas de forma necessária, proporcional, temporalmente limitada e sujeita ao escrutínio independente, para se evitar que decisões sobre matérias sensíveis quanto estas dependam de interpretações das partes interessadas.¹¹

Há também espaço para reforçar direitos hoje ausentes ou pouco abordados, como o direito à limitação do tratamento, o direito a não ficar sujeito a decisões exclusivamente automatizadas com efeitos

relevantes, a obrigação de explicabilidade em perfis de risco e crédito, e garantias específicas contra usos discriminatórios de dados biométricos e de inteligência artificial.¹²

te, time-limited and subject to independent scrutiny, in order to prevent decisions on such sensitive matters from depending on the interpretations of interested parties.

There is also room to strengthen rights that are currently absent or insufficiently addressed, such as the right to restriction of processing, the right not to be subject to solely automated decisions with significant effects, the obligation of explainability in

risk and credit profiling, and specific safeguards against discriminatory uses of biometric data and artificial intelligence.

5. Implementação e desafios de conformidade

Existem vários desafios que devem ser tidos em conta. Um deles será transformar deveres jurídicos em rotinas organizacionais. A obrigação de designar Encarregados de Protecção de Dados (EPD) em entidades públicas e privadas, tal como se propõe, poderá induzir ao mero cumprimento formal das exigências legais, caso a exigência não seja ajustada à natureza e dimensão das instituições, volume de dados e sensibilidade das operações de tratamento realizadas por cada organização. Para micro e pequenas organizações, bem como para entidades cujas actividades envolvam reduzidos riscos para os direitos dos titulares, a regulamentação deverá prever mecanismos de implementação proporcionais, preservando, em qualquer circunstância, o nível de protecção conferido aos titulares dos dados.¹³

O mesmo princípio deverá aplicar-se às restantes obriga-

ções organizacionais previstas na proposta, como a manutenção de registos das operações de tratamento de dados, a realização de avaliações de impacto e a adopção de políticas internas de protecção de dados. Embora estes deveres sejam fundamentais para promover uma gestão responsável da informação, a sua implementação exigirá orientações técnicas claras, modelos de referência, acções de capacitação e um período razoável de adaptação antes da aplicação plena do regime sancionatório.¹⁴

Existe, igualmente, uma inconsistência que merece atenção. O artigo 43 estabelece que a comunicação de incidentes a ANPD e ao titular ocorra cinco dias após conhecimento, enquanto o artigo 48 fixa notificação a autoridade de controlo no prazo de 72 horas. A lei deve adoptar um regime único ou distinguir claramente a notificação inicial a ANPD, da

5. Implementation and compliance challenges

There are several challenges that must be taken into account. One of them will be transforming legal duties into organizational routines. The obligation to designate Data Protection Officers (DPOs) in public and private entities, as proposed, could lead to merely formal compliance with legal requirements if the requirement is not adjusted to the nature and size of the institutions, the volume of data and the sensitivity of the processing operations carried out by each organization. For micro and small organizations, as well as for entities whose activities involve low risks to data subjects' rights, the regulations should provide for proportionate implementation mechanisms while preserving, in all circumstances, the level of protection afforded to data subjects.

The same principle should apply to the other organizational obligations provided for in the proposal, such as maintaining records of data processing

operations, carrying out impact assessments and adopting internal data protection policies. Although these duties are essential to promote responsible information management, their implementation will require clear technical guidance, reference models, capacity-building activities and a reasonable adaptation period before the sanctions regime is fully applied.

There is also an inconsistency that deserves attention. Article 43 establishes that incidents must be communicated to the ANPD and to the data subject five days after becoming known, while article 48 sets notification to the supervisory authority within 72 hours. The law should adopt a single regime or clearly distinguish initial notification to the ANPD from communication to the data subject, supplementary notification and incidents with no relevant risk.

In addition, it is our view that

11 Cf. artigo 25, nos 3 e 4; artigo 2, n.º 3, alínea e).

12 Cf. artigos 5, 16, 30, 45 e 46.

13 Cf. artigos 38, 39, 40 e 41.

14 Cf. artigos 45, 46, 53 e 54.

comunicação ao titular, notificação complementar e incidentes sem risco relevante.¹⁵

Adicionalmente, é nosso entendimento que a aprovação de uma lei, por si só, não garante a protecção efectiva dos dados pessoais. Um dos maiores desafios consiste na criação e funcionamento de uma autoridade de protecção de dados verdadeiramente independente, dotada de autonomia financeira, recursos humanos qualificados, capacidade técnica e poderes efectivos de fiscalização e sancionamento. Em muitos países, estas entidades enfrentam limitações orçamentais, escassez de especialistas e dificuldades em exercer controlo sobre organismos públicos e grandes empresas tecnológicas.¹⁶

O caso de Angola é ilustrativo. Embora a Lei da Protecção de Dados Pessoais (Lei n.º 22/11) esteja em vigor desde 2011 e exista a Agência de Protecção de Dados (APD), diversos estudos apontam que a autoridade tem enfrentado limitações institucionais e operacionais, reduzindo a capacidade de fiscalização sistemática e de aplicação efectiva das sanções previstas na lei. Situações semelhantes podem ser observadas em países como Cabo Verde e São Tomé e Príncipe, onde o principal desafio deixou de ser legislativo e passou a ser institucional.¹⁷

Outro desafio estrutural reside no baixo nível de literacia digital e de conhecimento sobre protecção de dados, tanto por parte dos cidadãos como das instituições públicas e privadas. Muitas organizações continuam a recolher, conservar e partilhar dados pessoais sem políticas claras de consentimento, segurança da informação, gestão de riscos ou resposta a incidentes de segurança. Paralelamente, muitos cidadãos desconhecem os seus próprios direitos, não reclamam quando estes são violados e continuam a aceitar práticas abusivas de tratamento de dados.

Este fenómeno é igualmente visível em Angola¹⁸, onde vários diagnósticos indicam que a conformidade com a Lei de Protecção de Dados permanece desigual entre sectores, sendo mais desenvolvida nas instituições financeiras e empresas de telecomunicações do que na administração pública ou em pequenas empresas. A mesma realidade verifica-se em diversos países africanos, onde a implementação da legislação depende de programas contínuos de sensibilização, formação de profissionais, certificação de encarregados de protecção de dados e campanhas públicas de educação digital.

the approval of a law, by itself, does not guarantee the effective protection of personal data. One of the greatest challenges lies in the creation and functioning of a truly independent data protection authority, endowed with financial autonomy, qualified human resources, technical capacity and effective supervisory and sanctioning powers. In many countries, these entities face budgetary limitations, a shortage of specialists and difficulties in exercising control over public bodies and large technology companies.

The case of Angola is illustrative. Although the Personal Data Protection Law (Law No. 22/11) has been in force since 2011 and the Data Protection Agency (APD) exists, several studies indicate that the authority has faced institutional and operational limitations, reducing its capacity for systematic supervision and effective application of the sanctions provided for by law. Similar situations can be observed in countries such as Cabo Verde and Sao Tome and Principe, where the main challenge has ceased to be legislative and has become institutional.

Another structural challenge lies in the low level of digital

literacy and knowledge about data protection among both citizens and public and private institutions. Many organizations continue to collect, retain and share personal data without clear policies on consent, information security, risk management or response to security incidents. At the same time, many citizens are unaware of their own rights, do not complain when those rights are violated and continue to accept abusive data processing practices.

This phenomenon is also visible in Angola, where several assessments indicate that compliance with the Data Protection Law remains uneven across sectors, being more developed in financial institutions and telecommunications companies than in the public administration or in small businesses. The same reality can be seen in several African countries, where the implementation of legislation depends on continuous awareness-raising programs, professional training, certification of data protection officers and public digital education campaigns.



¹⁵ Cf. artigo 43, n.os 5 e 6; artigo 48, n.os 1 a 5.

¹⁶ African Union. (2022). Malabo Convention on Cyber Security and Personal Data Protection.

¹⁷ Network of African Data Protection Authorities (NADPA). Relatórios institucionais.

¹⁸ CIPESA (Collaboration on International ICT Policy for East and Southern Africa). Diversos relatórios sobre privacidade e protecção de dados em África.

6. Considerações finais e recomendações

Importa reconhecer que a Proposta de lei não representará o ponto de chegada, mas sim o início de um processo contínuo de consolidação de uma cultura de protecção de dados em Moçambique. Os direitos previstos na referida Proposta apenas produzirão efeitos concretos se forem acompanhados por mecanismos eficazes de implementação, fiscalização e responsabilização. Tal exige uma autoridade de controlo independente, dotada de autonomia, recursos técnicos e capacidade sancionatória, bem como um investimento consistente na capacitação das instituições públicas, do sector privado e dos próprios cidadãos sobre os seus direitos e deveres em matéria de protecção de dados,

No geral, a Proposta de Lei de Protecção de Dados Pessoais

representa um avanço estrutural para a consolidação da transformação digital em Moçambique, ao estabelecer, pela primeira vez, um quadro jurídico abrangente para o tratamento de dados pessoais por entidades públicas e privadas. O instrumento legal preenche uma lacuna legislativa de um direito constitucionalmente previsto (entre outros, o artigo 41 da Constituição da República) e aproxima o país dos padrões internacionais nesta matéria. Todavia, a sua eficácia dependerá não apenas da qualidade das soluções jurídicas adoptadas, mas também da robustez da arquitectura institucional criada, da clareza das normas aprovadas e da capacidade dos diferentes actores em assegurar a sua implementação efectiva, havendo, por isso, a necessidade de:

Reforçar a independência institucional da Autoridade Nacional de Protecção de Dados (ANPD) - assegurando autonomia administrativa, financeira e operacional, regras transparentes de nomeação e cessação de funções, incompatibilidades, mecanismos adequados de prestação de contas e salvaguardas contra interferências externas. Paralelamente, importa delimitar de forma mais clara o papel do Conselho Nacional de Protecção de Dados Pessoais, reservando-lhe funções de coordenação estratégica, sem interferência nas competências regulatórias, fiscalizadoras e sancionatórias da ANPD.

Aperfeiçoar os mecanismos de protecção dos direitos fundamentais - clarificando as excepções relacionadas com segurança pública, defesa nacional, investigação criminal e interesse público, mediante critérios rigorosos de necessidade, proporcionalidade, finalidade específica, duração limitada e fiscalização independente. Recomenda-se igualmente a introdução de salvaguardas adicionais para decisões exclusivamente automatizadas, sistemas de inteligência artificial, perfilagem, biometria e outras tecnologias susceptíveis de produzir impactos significativos sobre os direitos e liberdades dos cidadãos.

6. Final considerations and recommendations

It is important to recognize that the bill will not represent the endpoint, but rather the beginning of a continuous process of consolidating a data protection culture in Mozambique. The rights provided for in the bill will produce concrete effects only if they are accompanied by effective implementation, oversight and accountability mechanisms. This requires an independent supervisory authority endowed with autonomy, technical resources and sanctioning capacity, as well as consistent investment in building the capacity of public institutions, the private sector and citizens themselves regarding their rights and duties in the field of data protection.

Overall, the Personal Data Protection Bill represents a structural step forward for the consolidation of digital transfor-

mation in Mozambique, by establishing, for the first time, a comprehensive legal framework for the processing of personal data by public and private entities. The legal instrument fills a legislative gap concerning a constitutionally recognized right (among others, article 41 of the Constitution of the Republic) and brings the country closer to international standards in this area. However, its effectiveness will depend not only on the quality of the legal solutions adopted, but also on the robustness of the institutional architecture created, the clarity of the rules approved and the capacity of the different actors to ensure their effective implementation. There is therefore a need to:

Strengthen the institutional independence of the National Data Protection Authority (ANPD) - ensuring administrative, financial and operational autonomy, transparent rules for appointment and termination of office, incompatibilities, adequate accountability mechanisms and safeguards against external interference. At the same time, it is important to define more clearly the role of the National Personal Data Protection Council, reserving for it functions of strategic coordination without interference in the ANPD's regulatory, supervisory and sanctioning powers.

Improve fundamental rights protection mechanisms - clarifying the exceptions related to public security, national defense, criminal investigation and public interest through rigorous criteria of necessity, proportionality, specific purpose, limited duration and independent oversight. It is also recommended that additional safeguards be introduced for solely automated decisions, artificial intelligence systems, profiling, biometrics and other technologies capable of producing significant impacts on citizens' rights and freedoms.

Adoptar um modelo de conformidade proporcional e baseado no risco - ajustando as obrigações impostas aos agentes de tratamento à natureza, dimensão e sensibilidade das operações realizadas. Esta abordagem permitirá reduzir encargos desnecessários para entidades de menor risco, sem comprometer a protecção dos titulares dos dados, favorecendo simultaneamente uma implementação mais eficiente e sustentável do novo regime jurídico.

Aperfeiçoar os mecanismos de protecção dos direitos fundamentais - clarificando as excepções relacionadas com segurança pública, defesa nacional, investigação criminal e interesse público, mediante critérios rigorosos de necessidade, proporcionalidade, finalidade específica, duração limitada e fiscalização independente. Recomenda-se igualmente a introdução de salvaguardas adicionais para decisões exclusivamente automatizadas, sistemas de inteligência artificial, perfilagem, biometria e outras tecnologias susceptíveis de produzir impactos significativos sobre os direitos e liberdades dos cidadãos.

Reforçar a segurança jurídica do sistema - harmonizando os procedimentos e prazos de notificação de violações de dados pessoais, clarificando as responsabilidades dos diferentes intervenientes e reduzindo potenciais ambiguidades interpretativas que possam dificultar a aplicação uniforme da futura lei.

Adopt a proportionate and risk-based compliance model - adjusting the obligations imposed on processing agents to the nature, scale and sensitivity of the operations carried out. This approach will make it possible to reduce unnecessary burdens for lower-risk entities without compromising the protection of data subjects, while also favoring a more efficient and sustainable implementation of the new legal regime.

Strengthen the legal certainty of the system - harmonizing the procedures and deadlines for notification of personal data breaches, clarifying the responsibilities of the different actors and reducing potential interpretive ambiguities that may hinder uniform application of the future law.

Implement the new regime gradually and with support - prioritizing timely preparation of complementary regulations, production of technical guidance, capacity building for public and private institutions, and adoption of compliance assistance mechanisms, especially for organizations with lower technical and financial capacity. A phased implementation will help consolidate a data protection culture based on prevention, accountability and continuous improvement.

