CARTILHA

CYBERBRICS: CYBERSECURITY REGULATIONS IN THE BRICS COUNTRIES

O projeto **CyberBRICS** busca mapear as abordagens dos países do grupo BRICS — **Brasil, Rússia, Índia, China e África do Sul** — no que diz respeito à regulação das tecnologias digitais, desenvolvendo uma análise comparativa das políticas digitais elaboradas pelos integrantes do grupo. Esse trabalho buscou oferecer um entendimento de como a cibersegurança é conceituada e estruturada nos países do BRICS, considerando que a segurança cibernética desempenha um papel fundamental no âmbito da transformação digital que está remodelando governos, economias e sociedades.

Essa mudança é acompanhada de riscos crescentes – como vazamentos de dados, ataques cibernéticos, fraudes digitais, entre outros – tonando particularmente útil o mapeamento dos marcos normativos que regulam as diversas dimensões da cibersegurança e das instituições responsáveis por implementar essas normas. A cartilha a seguir resume os principais achados da pesquisa e serve como ferramenta de referência para:

- Formuladores de políticas públicas e tomadores de decisão;
- Organizações da sociedade civil, setor privado e academia;
- Profissionais interessados na governança digital, particularmente no Sul Global.

O termo **BRICS** surgiu em 2001 como um conceito utilizado para destacar as economias emergentes com maior projeção de crescimento até 2030. Desde então, o acrônimo evoluiu num bloco político-institucional ativo, promovendo cooperação em áreas como economia, saúde, infraestrutura e, desde as revelações do Edward Snowden, tecnologias digitais.

POR QUE OS BRICS SÃO ESTRATÉGICOS NO DEBATE DIGITAL?

Representam mais de 40% da população mundial;

Representam mais de 40% dos usuários de internet, usam e produzem intensivamente tecnologias digitais;

Exercem crescente influência sobre as regras globais que impactam tecnologias digitais, particularmente no que diz respeito à governança de dados e cibersegurança.

A disposição do BRICS em cooperar se expandiu para o campo das normas e padrões internacionais, como destacado a partir da Declaração de Xiamen em 2017, que indicou o compromisso dos países com o estabelecimento conjunto de regras internacionalmente aplicáveis para a segurança de infraestrutura de TIC e proteção de dados. Esta cooperação resultou no esforço conjunto para a elaboração de uma Convenção da ONU sobre Cibercrime, adotada em 2024.

POR QUE FOCAR NA CIBERSEGURANÇA?

A expansão e redução de custos da conectividade permitem que governos e empresas ofereçam uma ampla gama de serviços com mais eficiência do que nunca, criando oportunidades sociais e econômicas incríveis por meio das tecnologias digitais. No entanto, ao mesmo tempo, essas tecnologias possibilitam ameaças cibernéticas, crimes cibernéticos e ataques cibernéticos que limitam os benefícios prometidos pelas tecnologias digitais e criam uma ampla gama de externalidades negativas que precisam ser enfrentadas com políticas e regulamentações sólidas.

Por isso, a cibersegurança tornou-se uma preocupação primordial para todos os países dos BRICS. Como destacado na introdução do livro, **a cibersegurança pode ser metaforicamente comparada à** mudança climática, isto é um fenômeno transnacional, cujos riscos demandam um pensamento sistêmico e exigem uma coordenação global. Ela é um dos campos mais sensíveis da política pública digital. Ainda que invisível para grande parte da população, a cibersegurança tem impactos profundos em:

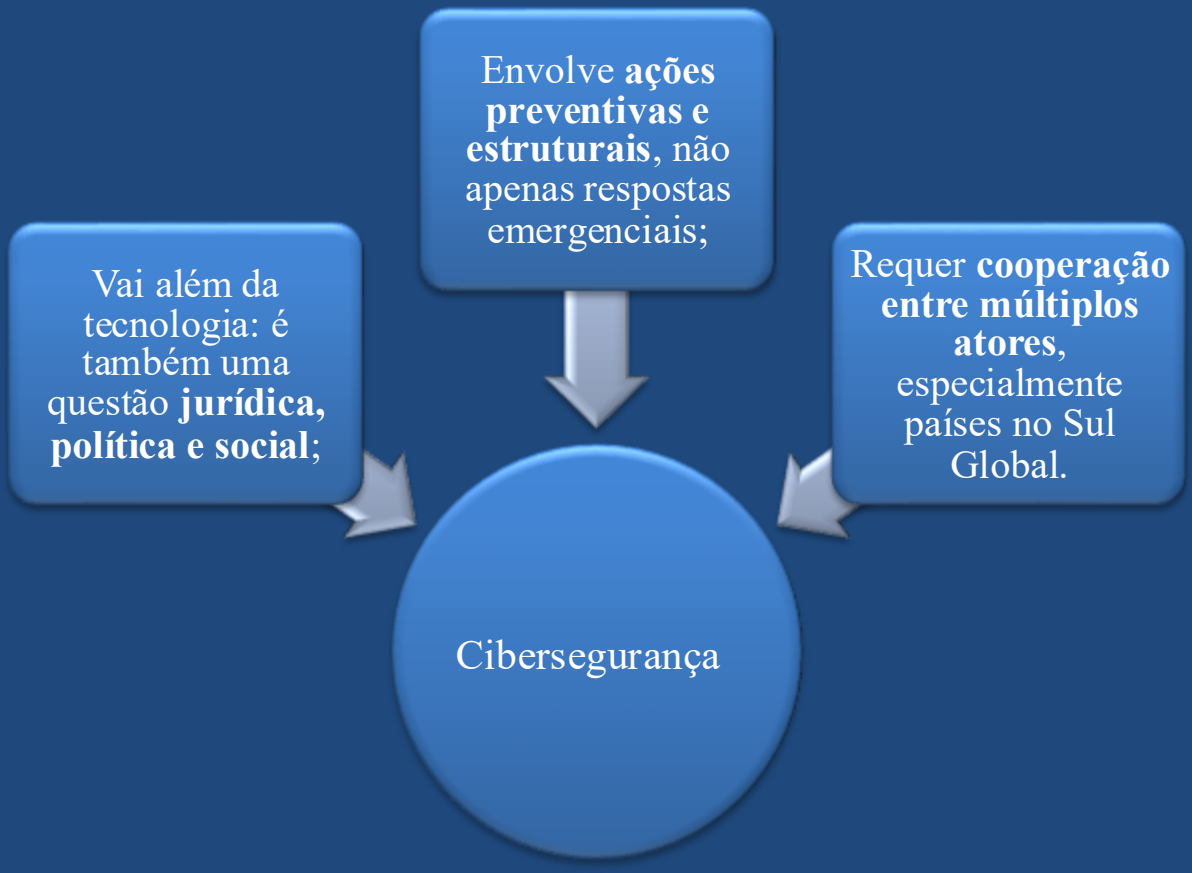
Soberania nalcional, ao permitir o funcionamento regular das infraestruturas críticas e serviços essenciais;

Direitos fundamentais, ao empoderar e proteger indivíduos com o objetivo de facilitar o pleno gozo de direitos e liberdades ao usar tecnologias digitais;

Confiança no estado e nas instituições públicas, ao preservar processos democráticos de ataques e manipulações;

POR QUE FOCAR NA CIBERSEGURANÇA?

A abordagem adotada no âmbito do projeto CyberBRICS parte do princípio de que cibersegurança:



OS PILARES DA PESQUISA

A pesquisa CyberBRICS parte da análise comparativa de cinco dimensões consideradas como fundamentais para as políticas públicas de cibersegurança.

1. Proteção de Dados Pessoais

Com o crescimento acelerado da Internet e a massiva adoção de smartphones e dispositivos conectados (a chamada Internet das Coisas), os dados pessoais passaram a ser coletados de forma contínua, em larga escala. Isso oferece oportunidades para inovação e desenvolvimento, mas também representa riscos sérios para a privacidade e proteção de dados pessoais.

Nos BRICS, ficou claro que dados pessoais são um recurso estratégico. A garantia da proteção e da segurança de dados não é só um direito individual, mas uma questão de interesse nacional, essencial para o funcionamento dos governos, das economias e das sociedades como um todo.

Alguns dos avanços mais relevantes nos países do BRICS incluem:

- Brasil: Aprovação da LGPD e criação da Autoridade Nacional de Proteção de Dados (ANPD);
- Rússia: Regras rígidas de segurança e localização de dados dentro do território nacional;
- Índia: Privacidade reconhecida como direito fundamental pela Suprema Corte, e elaboração da nova lei de proteção de dados;
- China: Reforço legal com o Código Civil, Lei de Cibersegurança e regulações detalhadas sobre tratamento seguro de dados;
- África do Sul: Criação de autoridade reguladora de dados e entrada em vigor da Lei de Proteção de Informações Pessoais (POPIA).

2. Proteção do Consumidor Online

A digitalização dos mercados transformou profundamente as relações entre consumidores e fornecedores. Com plataformas digitais, e-commerce e dispositivos conectados, os consumidores enfrentam novas vulnerabilidades — desde vazamentos de dados até produtos inseguros e mal protegidos.

A rápida expansão da Internet das Coisas torna cada "coisa" um possível ponto de coleta de dados e, também, uma porta de entrada para ataques, configurando-se uma vulnerabilidade em potencial que pode ser explorada por agentes mal-intencionados. Portanto, o livro sustenta que regras solidas de proteção do consumidor são essenciais para reduzir as vulnerabilidades e incrementar a segurança de produtos e serviços. Particularmente, duas áreas complementares desempenham um papel instrumental para fortalecer uma normativa solida de proteção do consumidor:

- Fomentar a **educação do consumidor** e a **conscientização sobre riscos cibernéticos**;
- Implementar a incorporação de sistema de segurança no design dos produtos ou serviços conectados;

3. Cibercrime

Cibercrime envolve crimes cometidos **por meio ou em face de tecnologias da informação e comunicação (TICs).** Ataques cibernéticos, invasões, fraudes digitais, disseminação de malwares e crimes contra dados são cada vez mais comuns — e quase sempre ultrapassam fronteiras nacionais.

A ONU e a União Internacional de Telecomunicações (UIT) reconhecem que **cibercrime é parte integrante da cibersegurança**. Considerando que as ameaças cibernéticas raramente são nacionais, mas geralmente possuem natureza transfronteiriça, os BRICS têm buscado caminhos para harmonizar suas legislações e **reforçar a cooperação internacional**.

Nessa perspectiva, o surgimento de um marco jurídico compartilhado, que possa complementar a Convenção de Budapeste do Conselho da Europa foi considerada como uma prioridade comum para os países do grupo. O livro analisa as normativas nacionais e as iniciativas que vêm explorando crescentemente opções para aprofundar a cooperação dos membros por meio do Grupo de Trabalho dos BRICS sobre Segurança no Uso das TICs.

4. Ordem Pública no Espaço Digital

A "ordem pública" é um conceito amplo e, por vezes, vago, mas está no centro da regulação estatal sobre o que é permitido ou proibido no ambiente offline bem como online. Por essa razão, sua preservação deve ser perseguida dentro de marcos específicos do Estado de Direito, que definam quando é apropriado invocar a ordem pública como justificativa legítima e quais autoridades podem exercer funções de polícia, e em quais circunstâncias.

Nesta perspectiva, o volume mapeia as abordagens dos países do BRICS, considerando que a proteção e a preservação da ordem pública estão no centro das atividades de polícia administrativa, cujos objetivos são únicos em cada país. Por outro lado, a polícia judiciária possui caráter repressivo, voltado para o registro de infrações penais, coleta de provas e busca pelos autores de delitos específicos. Ambas as dimensões são analisadas no que diz respeito a seus desdobramentos digitais, destacando que:

Em muitos casos, intermediários privados — como redes sociais ou plataformas de hospedagem — são chamados a colaborar com o cumprimento da lei;

Os países BRICS integram essa dimensão em seus marcos regulatórios, criando funções que podem ser definidas como de polícia administrativa e judiciária para atores privados.

5. Ciberdefesa

Ciberdefesa é o braço militar e estratégico da cibersegurança. Envolve ações estatais não somente de proteção mas também de reação as ameaças cibernéticas, especialmente quando essas ameaças sejam direcionadas contra alvos críticos como serviços públicos digitais, e infraestrutura críticas de finanças, energia, comunicação, etc.

No BRICS, a ciberdefesa está majoritariamente sob comando de instituições militares ou de inteligência, com alto grau de sigilo. Isso dificulta a análise pormenorizada, mas permite a identificação de alguns padrões visíveis:

- FOCO EM DOIS EIXOS: DEFENSIVO: PREVENÇÃO E RESILIÊNCIA DE SISTEMAS CRÍTICOS; E OFENSIVO: COMBATE À ESPIONAGEM E AÇÕES DE CONTRA-ATAQUE.
- FORMULADA PELO PODER EXECUTIVO, POR MEIO DE COMANDOS ESPECIAIS, GERALMENTE CRIADOS NO ÂMBITOS DOS MINISTÉRIOS DA DEfESA;

POR QUE ESSES PILARES SÃO IMPORTANTES?

Esses cinco eixos ajudam a compreender como cada país dos BRICS estrutura sua política pública e suas regulações de cibersegurança — e até que ponto esses elementos convergem ou divergem. A pesquisa foca nos **marcos legais e institucionais**, sem abordar ferramentas técnicas ou práticas do setor privado. O objetivo é fornecer um mapa comparativo das políticas digitais que estão moldando a evolução das lideranças do Sul Global — e oferecer insumos concretos para tomadores de decisão.

CONCLUSÃO E CAMINHOS FUTUROS

Como evidenciado na conclusão do volume, os países do BRICS vêm trilhando um caminho de convergência prática, com avanços importantes em diversas frentes, enquanto constroem sua soberania digital de maneira mais ou menos coordenada com suas abordagens de cibersegurança. A digitalização acelerada das economias, dos serviços públicos e da vida cotidiana exige ações firmes para prevenir e responder a ameaças como ataques cibernéticos, espionagem digital, vazamento de dados e circulação de conteúdos ilícitos.

Garantir a segurança de infraestruturas críticas, sistemas de informação e bases de dados nacionais é, hoje, uma questão de soberania. As abordagens dos países do BRICS oferecem uma ilustração interessante de como as maiores economias da do Sul Global estão lidando com esses desafios.

Quer saber mais? Acesse o estudo completo: