O IMPACTO DA TECNOLOGIA DA INFORMAÇÃO NA SEGURANÇA PÚBLICA CONTEMPORÂNEA

Humberto de Sá Garay

Em meio a plena Era Digital na qual nos encontramos imersos, as tecnologias da informação (TI) já ocupam o epicentro estratégico para a execução de políticas de segurança pública eficientes, seja na vertente de inteligência, seja na de investigação criminal.

VOLUME, VELOCIDADE DE PRODUÇÃO E ARMAZENAMENTO DE DADOS

Isso se deve às necessidades institucionais da segurança púbica de fazer frente à explosão informacional promovida pela Terceira Revolução Industrial, caracterizada pela expansão do volume e velocidade da produção e armazenamento de dados a índices cada vez maiores – e outrora inimagináveis.

DESENVOLVIMENTO CONTÍNUO DE METODOLOGIA

Em tal contexto, a principal dessas necessidades parece ser a de desenvolvimento e constante aperfeiçoamento de uma metodologia especializada para o aumento da capacidade de obter e analisar eficazmente o enorme conjunto de dados provenientes da complexa realidade cibernética, completamente distinta da metodologia tradicional, projetada até então, para um mundo preponderantemente analógico.

DESAFIO INFORMACIONAL DA SEGURANÇA PÚBLICA CONTEMPORÂNEA: MUITOS DADOS, POUCA INFORMAÇÃO E ESCASSO CONHECIMENTO

Assim, na segurança pública contemporânea, o desafio informacional, geralmente, é extrair significados úteis e confiáveis de uma infinita massa de dados que ~~se~~ constituem o típico e conhecido *Big Data*: uma massa de dados advindos de múltiplas fontes, com diferentes estruturas binárias, com tamanhos cada vez maiores e organizados de modos diferentes. Sem isso, o que restará para a segurança pública é a incapacidade operativa ante a produção massiva de insumos informacionais, ficando presa em um cenário de *muitos dados, mas pouca informação*.

METODOLOGIA HÍBRIDA E INTEGRADA PARA A INTELIGÊNCIA DE DADOS

Essa metodologia é conceituada, por alguns, como Inteligência de Dados, um processo de produção de conhecimento a partir de múltiplas fontes, de diversos dispositivos, provedores de aplicações e de acesso ou ainda, de sistemas de informática com grandes volumes de dados dispersos no ambiente cibernético – computação em nuvem. É certo que a metodologia dessa espécie de Inteligência depende do emprego de tecnologias da informação de alta performance que conglobe, no mínimo, três dimensões logicamente concatenadas: 1. Obtenção: que se traduz na mais ampla capacidade de *input* informacional, para obter dados – artefatos, oriundos das mais diversas fontes e com os mais variados formatos lógicos. 2. Processamento: que corresponde a capacidade de reconhecer, armazenar e organizar os diversos tipos de dados, que podem ser estruturados[1] ou não estruturados[2]. 3. Análise: que é a possibilidade de integração de base de dados diferentes, com cruzamentos, correlações, análises de vínculos e representações gráficas, tudo calcado em Inteligência Artificial, monitoramento em tempo real e por várias equipes integradas.

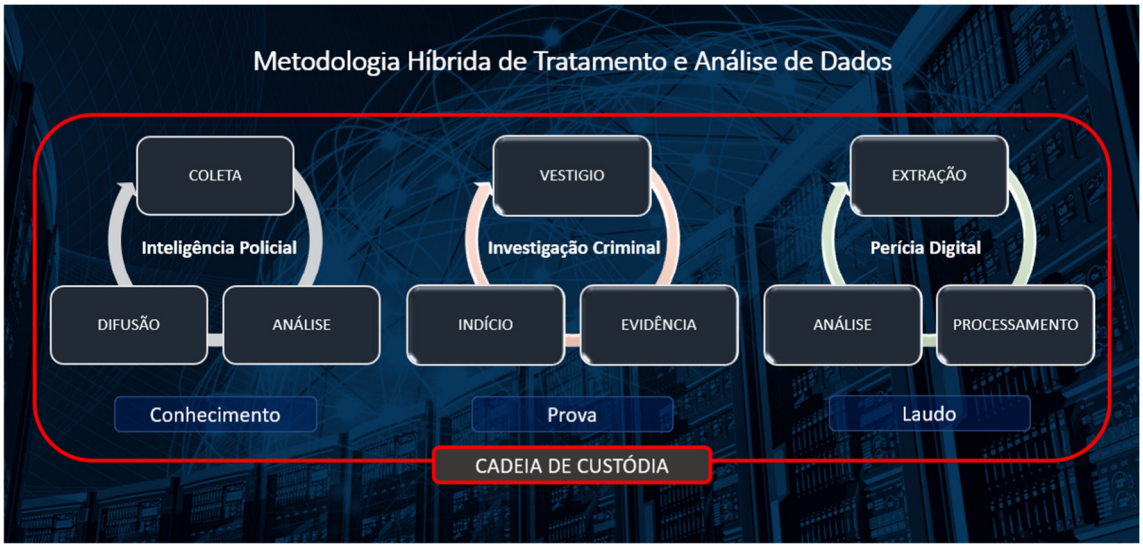

Figura do autor: Design da metodologia híbrida e integrada para tratamento e análise de dados para a segurança pública contemporânea aplicados a inteligência e investigação criminal, considerando os ciclos e procedimentos operacionais padrão de cada atividade.

Em conjunto a essa necessidade de obtenção e análise, é inevitável a correspondente proteção implacável dos dados, pois, do contrário, é melhor que nem sejam produzidos

[1] Os **dados estruturados** são aqueles organizados e representados com uma estrutura rígida, a qual foi previamente planejada para armazená-los, por exemplo um banco de **dados**, que é a representação mais típica e comum de **dados estruturados**.

[2] Os **dados não estruturados** não podem ser organizados em tabelas e campos específicos. Incluímos aí, informações como, comentários em redes sociais, e-mails, vídeos, imagens, textos diversos, entre outros.

por medidas de segurança. Para tanto, a metodologia deve conter, em si mesma, do início ao fim, medidas defensivas que resguardem o dado durante todo o seu ciclo de vida, garantindo a segurança do seu tratamento.

SEGURANÇA DA INFORMAÇÃO

Os incidentes de comprometimento ou vazamento de dados obtidos no interesse da segurança pública, podem ensejar a antecipação e neutralização das ações estatais por parte de agentes criminosos e, até mesmo, a exposição de da identidade de servidores da segurança, vítimas ou testemunhas colocando-os em risco e ainda desperdiçar todo o esforço investigativo.

Isso é reforçado pela louvável e necessária cultura de proteção de dados pessoais, alavancada pela edição da Lei Geral de Proteção de Dados (LGPD). As atividades de segurança pública invariavelmente lidam com nomes e prenomes, números de documentos pessoais, endereços de emails, números telefônicos, endereços de *IP*, antecedentes criminais, dentre muitos outros. Tais dados representam, em última análise, o exercício das liberdades individuais e, por isso, exigem proteção efetiva e somente podem ser relativizados de forma proporcional, para atender a finalidades públicas, dentre as quais a de segurança pública.

No caso específico de investigações criminais, a proteção ganha contornos ainda mais especiais, já que a legislação processual penal condiciona a validade das provas penais, objetivo últimos dessas apurações persecutórias, a preservação da cadeia de custódia que demonstre sua perfeita integridade, via registro cronológico do manuseio de vestígios de crime (inclusive os digitais), livre de quaisquer alterações, maliciosas ou não.

Por isso tudo, a eficácia da segurança pública é cada vez mais dependente da inovação tecnológica e pelo constante estudo técnico-científico em busca das melhores práticas possíveis.