CÂMARA DOS DEPUTADOS

PROJETO *DE* LEI Nº , DE 2015
(Do Sr. Rômulo Gouveia)

Altera a Lei nº 9.503, de 23 de setembro de 1997, para dispor sobre segurança cibernética de veículos.

O Congresso Nacional decreta:

Art. 1º Esta Lei altera a Lei nº 9.503, de 23 de setembro de 1997, que instituiu o Código de Trânsito Brasileiro, para dispor sobre segurança cibernética de veículos.

Art. 2º O art. 103 da Lei nº 9.503, de 1997, passa a vigorar com a seguinte redação:

"Art. 103. .....
§ 1º.....
.....

§ 3º Os fabricantes, montadores e importadores de veículos deverão empregar as melhores práticas de segurança para proteger sistemas de softwares críticos, bem como pontos de entrada para sistemas eletrônicos, dos ataques de hackers.

§ 4º O CONTRAN deverá estabelecer os procedimentos para avaliação de vulnerabilidades aos ataques de hackers, tipos de testes de integridade de sistemas eletrônicos e o cronograma de incorporação das medidas de segurança cibernética aos novos projetos de veículos." (NR)

Art. 3º Acrescente-se o seguinte artigo à Lei nº 9.503, de 1997:

> "Art. 309-A. Comprometer o funcionamento de sistemas de software críticos ou sistemas eletrônicos veiculares, ou ainda, expor ao perigo motorista por meio de acesso não autorizado a controles eletrônicos ou dados de condução.
>
> Penas – detenção, de seis meses a um ano, ou multa."

Art. 4º O Anexo I da Lei nº 9.503, de 1997, passa a vigorar acrescido das seguintes definições:

> "DADOS DE CONDUÇÃO – qualquer informação eletrônica recolhida sobre o veículo, incluindo localização, velocidade, informações sobre proprietário, arrendatário, motorista ou passageiro.
>
> HACKERS – indivíduos que obtém acesso não autorizado a controles eletrônicos ou dados de condução, a partir de uma conexão remota, sem fio, ou por meio de conexões com fio.
>
> PONTOS DE ENTRADA – incluem sinais de controle que possam ser enviados ou recebidos de forma remota ou por meio de conexões físicas.
>
> SISTEMAS DE SOFTWARES CRÍTICOS – sistemas que podem afetar ou comprometer o controle do motorista sobre o movimento dos veículos."

Art. 5º Esta Lei entra em vigor na data de sua publicação.

JUSTIFICAÇÃO

Sistemas eletrônicos, sensores e a computação de forma geral estão a serviço da indústria automobilística com possibilidades concretas de contribuir para a redução do número de acidentes e das perdas humanas e econômicas decorrentes.

O emprego de tecnologias de segurança, tais como sensores de detecção de colisão frontal, frenagem automática de emergência, e tecnologias de comunicação de acidentes, pode ser a diferença para preservar a vida de milhares de motoristas.

Com o avanço da tecnologia, as pessoas e as corporações começaram a se familiarizar com o conceito de segurança cibernética. Ao longo das últimas décadas, nossas vidas foram revolucionadas pela conectividade rápida, possível graças a computadores, Internet, satélites e outras tecnologias. Os ataques cibernéticos evoluíram na mesma velocidade.

A segurança cibernética surge, então, da necessidade de proteger sistemas vitais e as informações neles contidas. Aplicado aos veículos, a segurança cibernética assume um papel ainda mais importante: sistemas e componentes que regem a segurança devem ser protegidos contra ataques maliciosos, acessos não autorizados, danos ou qualquer outra coisa que possa interferir com as funções de segurança.

Paradoxalmente, os fabricantes de veículos, ao tempo em que investem milhões no desenvolvimento de tecnologias de suporte ao motorista, minimizam o risco de ataques de hackers aos sistemas veiculares, ignorando as ameaças decorrentes da conectividade. No entanto, graças aos trabalhos de vários pesquisadores, restou comprovado que é fácil se conectar a rede interna de um veículo,

introduzir comandos para controlar faróis, janelas, e pior, freios e direção.

É por esta razão, que a segurança cibernética em veículos não pode ser ignorada por esta Casa Legislativa. O debate acerca da questão é essencial para a aceitação pública dos sistemas dos veículos e da tecnologia de segurança.

Pelo projeto, os fabricantes, montadores e importadores de veículos deverão empregar as melhores práticas de segurança para proteger sistemas de softwares críticos, bem como pontos de entrada para sistemas eletrônicos, dos ataques de hackers. Os procedimentos para avaliação de vulnerabilidades aos ataques de hackers, tipos de testes de integridade de sistemas eletrônicos e o cronograma de incorporação das medidas de segurança cibernética aos novos projetos de veículos deverão ser estabelecidos pelo Contran. Além disso, está prevista a penalidade para quem, deliberadamente, acessa de forma indevida sistemas veiculares.

Entendo que o projeto ora apresentado procura agir tempestivamente na mitigação dos riscos decorrentes da vulnerabilidade dos sistemas inteligentes dos veículos, contribuindo para a segurança dos usuários, razão pela qual, trago à consideração dos ilustres Pares, na expectativa de sua aprovação.

Sala das Sessões, em de de 2015

Deputado **RÔMULO GOUVEIA**
PSD/PB