



**ExpressoLivre - ExpressoMail**

Enviado por: "Ciber crimes" <ciber Crimes@pc.pr.gov.br>

De: ciber Crimes@pc.pr.gov.br

Para: emersonbd@ufrj.br

Data: 08/06/2021 17:53 (21 minutos atrás)

Assunto: Re: Fw: Protocolo Ouvidoria PC-PR 61086/2021 - Apoio em pesquisa acadêmica - UFRRJ  

Anexos: | RESOLUÇÃO 293\_05.pdf (12 KB) | EX\_2005-11-23.pdf (668 KB)

Prezado Emerson,

Seguem algumas respostas aos seus questionamentos. Para outras, não temos ferramentas para tais filtros e o local onde podem ser encontrados foram indicados nas respostas.

1. Qual a história de criação da unidade? **Demanda de ciber crimes no Estado do Paraná. Criado em 2005 pela resolução SESP 293/05, em anexo.**
2. Qual a formação e composição dos seus quadros funcionais? Existem apenas profissionais da segurança pública ou são contratados consultores? **Somente profissionais de segurança pública.**
3. Quais os treinamentos (em tecnologia) necessários e/ou disponíveis para que sejam parte da unidade? **Preferência conhecimento em direito e TI.**
4. Existem ferramentas que tenham sido desenvolvidas internamente? Quem faz o apoio e suporte de TI? **Não foram desenvolvidas ferramentas internamente. A demanda gigantesca versus o pouco efetivo não nos possibilita tais estudos. Apoio e suporte de TI feitos pelo setor de informática da PC-PR e pela empresa pública CELEPAR.**
5. Existe um perfil profissional específico ou desejado para se trabalhar numa unidade desse tipo? **Preferencialmente com formação em direito e TI.**
6. Qual o número de registros de ocorrência por mês? **Por volta de 1000 em 2021.** Quantas são lavradas na própria unidade? **Não temos como filtrar esse dado na unidade. Favor entrar em contato com o CAPE da SESP-PR para que façam a coleta via sistema BI.** Quantas são online? **Mesma resposta anterior.** É possível ter uma ocorrência oriunda de outras unidades da estrutura de segurança pública? **Sim. O Nuciber presta apoio ao Estado do Paraná todo.**
7. Existe uma estatística sobre o tempo médio de uma investigação considerando a abertura de uma ocorrência e sua conclusão? **Não. Dependemos em grande maioria de quebras de sigilo que envolvem o poder judiciário e respostas de provedores de aplicação e conexão. Não há estatísticas sobre tempo médio de investigação.**
8. Existem trabalhos ou mapas de análise estatística do tipo "Mancha Criminal"? Talvez algum tipo de abordagem por tipo de crime e frequência de determinados tipos de ocorrência p.ex.? **Entre em contato com o CAPE da SESP-PR.**
9. Dentre os vários crimes elucidados certamente existem aqueles de maior destaque e que viraram casos de estudo e análise. Poderiam ser citados e resumidas algumas dessas ações? **Ações de combate à pedofilia na internet. Pesquise sobre Operação Luz na Infância. O NUCIBER coordena essa operação no Paraná.**
10. A unidade faz ações educacionais ou patrocina ações de prevenção ou monitoração de crimes digitais ou ciber crimes? **Não. Trabalhamos sob demanda de registro de Boletim de Ocorrências.**
11. A unidade faz consultoria para outros órgãos de governo ou da iniciativa privada na parte de segurança da informação ou na parte de tecnologia de prevenção a crimes digitais? **Não.**

### Sobre Crimes Digitais:

1. Existem dados (Bancos de dados ou microdados) que possam ser analisados para fins estatísticos? Como posso solicitar uma cópia ou acesso? **Entre em contato com o CAPE da SESP-PR.**
2. Quais são os Modus Operandi mais comuns? Quais os crimes mais denunciados? **Crimes contra o patrimônio.**
3. Qual o típico perfil do criminoso? **Não há**

4. Existem indicativos de organizações criminosas “tradicionais” migrando para atuar nesse tipo de crime? **Não**
5. Existe um levantamento sobre o perfil das vítimas? **Não há**
6. Existe uma tabela com a tipificação dos crimes? **Código Penal como um todo e legislação penal esparsa**
7. A tipificação (tipificação criminal de delitos informáticos –Lei nº 12.737, de 30 de novembro de 2012) é suficiente para os casos ou é necessário fazer também um trabalho de analogia com os outros tipos de crime previstos no código penal para a devida instrução processual e apresentação de denúncia? **A referida lei representa uma parcela muito pequena de crimes que podem ser praticados pela internet. Como respondido na pergunta 6, é usado todo o código penal e legislação penal esparsa para enquadrar as condutas.**
8. Como se combatem as quadrilhas virtuais e como fica a tipificação criminal frente aos diferentes tipos de ações e responsabilidades? Existem casos que possam ser analisados (Por exemplo: Quem faz o vírus, quem faz o site ou hospeda o site para golpes, quem compartilha, quem usa a máquina infectada, quem recebe e repassa o ganho ilícito)? **Não fazemos essa análise devido à demanda de registros de Boletim de Ocorrência.**
9. Como é tratada a divulgação de crimes realizados para recrutamento por facções ou por demonstração de força? **Não temos casos dessa natureza no NUCIBER.**
10. Qual é o protocolo de combate a divulgação, venda e entrega de armas, drogas e entorpecentes? Existem casos que possam ser analisados? **Não temos casos relevantes no NUCIBER desta natureza. São tratados pelo DENARC.**

Sobre os aspectos jurídicos nos crimes via web:

1. Como é resolvida ou tratada a questão da jurisdição em investigações de crimes que são ou podem ser executados em vários locais pelo mundo (Estado/Brasil/Mundo)? **Segue-se jurisprudência/súmulas dos tribunais superiores.**
2. Existem acordos de cooperação policial no Brasil para esse tipo de crime? Qual o protocolo adotado para se acionar outras forças da área de segurança? **Via POLINTER**
3. Caso o Brasil venha a aderir, qual a expectativa sobre a aplicação da “Convenção de Budapeste” no referente ao combate ao cibercrime e ao crime digital?
4. A lei 13.964/2019 (Lei Anticrime), que possibilitou a infiltração virtual de agentes policiais para obter dados de conexão e cadastrais de membros de organizações envolvidas com crimes cibernéticos já foi usada em algum caso? Podem ser resumidas para ilustração? **Não foi aplicada ainda nos casos do NUCIBER.**
5. Imaginando que a unidade tem participação na Estratégia Nacional de Segurança Cibernética (batizada de "E-Ciber" por meio do decreto 10.222), já existem ações efetivas que possam ser destacadas? **Não**
6. Entre os casos de sucesso, existem histórias de ações conjuntas com outras unidades policiais do BRASIL ou do mundo em ações de combate ao cibercrime e crime digital? **Participação na Operação Luz na Infância (combate à pedofilia) e 404 (combate a violação de direitos autorais), ambas nacionais.**
7. Tendo as empresas privadas de tecnologia como a Google e Microsoft entre outras, além de ONGs (SaferNet p.ex.) exercido um papel expressivo no combate e sobretudo na denúncia de crimes pela internet, como é a cooperação com a iniciativa privada? Existem protocolos definidos? **No que tange aos crimes de exploração sexual de menores, tais empresas informam a Polícia Federal, que pode repassar as informações aos Estados onde pode se encontrar o criminoso.**
8. Existem eventos do tipo “Lei 9099” (Baixo Potencial Ofensivo) que podem ser ou foram resolvidos por Termos Circunstanciados com o escopo dos crimes digitais? **A grande maioria dos crimes contra a honra e demais crimes cibernéticos cuja pena seja inferior a 2 anos.**

Atenciosamente,

**PCPR****Núcleo de Combate aos  
Cibercrimes - NUCIBER**41 3304-6800 | [cibercrimes@pc.pr.gov.br](mailto:cibercrimes@pc.pr.gov.br)

Rua Pedro Ivo, 672 - Centro

Curitiba - PR | CEP 80010-020

Polícia Civil do Paraná alerta que esta mensagem pode conter informações pessoais e/ou sigilosas. Se você não for o destinatário ou a pessoa autorizada a receber esta mensagem, não deverá utilizar, copiar, alterar, divulgar a informação nela contida ou tomar qualquer ação baseada nessas informações. Se você recebeu esta mensagem por engano, por favor avise imediatamente o remetente, respondendo o e-mail e em seguida apague-o.

Em 27/05/2021 às 10:58 horas, "Ciber crimes" <[cibercrimes@pc.pr.gov.br](mailto:cibercrimes@pc.pr.gov.br)> escreveu:

**PCPR****Núcleo de Combate aos  
Cibercrimes - NUCIBER**41 3304-6800 | [cibercrimes@pc.pr.gov.br](mailto:cibercrimes@pc.pr.gov.br)

Rua Pedro Ivo, 672 - Centro

Curitiba - PR | CEP 80010-020

Polícia Civil do Paraná alerta que esta mensagem pode conter informações pessoais e/ou sigilosas. Se você não for o destinatário ou a pessoa autorizada a receber esta mensagem, não deverá utilizar, copiar, alterar, divulgar a informação nela contida ou tomar qualquer ação baseada nessas informações. Se você recebeu esta mensagem por engano, por favor avise imediatamente o remetente, respondendo o e-mail e em seguida apague-o.

----- Mensagem encaminhada -----

Remetente: "Emerson de Barros Duarte" <[emersonbd@ufrj.br](mailto:emersonbd@ufrj.br)>

Data: 26/05/2021 15:03

Assunto: Protocolo Ouvidoria PC-PR 61086/2021 - Apoio em pesquisa acadêmica - UFRRJ

Para: [cibercrimes@pc.pr.gov.br](mailto:cibercrimes@pc.pr.gov.br)

Bom Dia.

Seguindo orientação da Ouvidoria da PC-PR com protocolo 61086/2021, agradeço a disponibilidade de me atender e abaixo reapresento alguns questionamentos e a justificativa para tal incômodo.

Meu nome é Emerson Duarte (CPF 013330307/11 - Celular 21 991221370), sou aluno do curso de mestrado em humanidades digitais na Universidade Federal Rural do RJ (Atestado de matrícula em anexo) e minha área de pesquisa se concentra em métodos computacionais em políticas públicas e, em específico,

busco informações sobre cibercrimes e crimes digitais ou virtuais. Basicamente meu contato é por necessitar de mais informações para entender essa tipificação de crimes combatidos pelo sistema de segurança pública e seus desafios.

Minha proposta é trazer a visão do agente de segurança pública e os desafios que o mesmo enfrenta na investigação e no combate aos crimes digitais/cibernéticos, dissertando inclusive sobre a questão da legislação envolvida e suas eventuais limitações.

Abaixo eu tomo a liberdade de apresentar uma série de perguntas que podem vir a me ajudar nesse estágio inicial de levantamento de informações que imagino possa ser respondida por vocês ou que possam me indicar a quem devo submeter esse desafio.

#### Sobre unidades especializadas no combate aos crimes cibernéticos:

1. Qual a história de criação da unidade?
2. Qual a formação e composição dos seus quadros funcionais? Existem apenas profissionais da segurança pública ou são contratados consultores?
3. Quais os treinamentos (em tecnologia) necessários e/ou disponíveis para que sejam parte da unidade?
4. Existem ferramentas que tenham sido desenvolvidas internamente? Quem faz o apoio e suporte de TI?
5. Existe um perfil profissional específico ou desejado para se trabalhar numa unidade desse tipo?
6. Qual o número de registros de ocorrência por mês? Quantas são lavradas na própria unidade? Quantas são online? É possível ter uma ocorrência oriunda de outras unidades da estrutura de segurança pública?
7. Existe uma estatística sobre o tempo médio de uma investigação considerando a abertura de uma ocorrência e sua conclusão?
8. Existem trabalhos ou mapas de análise estatística do tipo “Mancha Criminal”? Talvez algum tipo de abordagem por tipo de crime e frequência de determinados tipos de ocorrência p.ex.?
9. Dentre os vários crimes elucidados certamente existem aqueles de maior destaque e que viraram casos de estudo e análise. Poderiam ser citados e resumidas algumas dessas ações?
10. A unidade faz ações educacionais ou patrocina ações de prevenção ou monitoração de crimes digitais ou cibercrimes?
11. A unidade faz consultoria para outros órgãos de governo ou da iniciativa privada na parte de segurança da informação ou na parte de tecnologia de prevenção a crimes digitais?

#### Sobre Crimes Digitais:

1. Existem dados (Bancos de dados ou microdados) que possam ser analisados para fins estatísticos? Como posso solicitar uma cópia ou acesso?
2. Quais são os Modus Operandi mais comuns? Quais os crimes mais denunciados?
3. Qual o típico perfil do criminoso?
4. Existem indicativos de organizações criminosas “tradicionais” migrando para atuar nesse tipo de crime?
5. Existe um levantamento sobre o perfil das vítimas?
6. Existe uma tabela com a tipificação dos crimes?
7. A tipificação (tipificação criminal de delitos informáticos –Lei nº 12.737, de 30 de novembro de 2012) é suficiente para os casos ou é necessário fazer também um trabalho de analogia com os outros tipos de crime previstos no código penal para a devida instrução processual e apresentação de denúncia?
8. Como se combatem as quadrilhas virtuais e como fica a tipificação criminal frente aos diferentes tipos de ações e responsabilidades? Existem casos que possam ser analisados (Por exemplo: Quem faz o vírus, quem faz o site ou hospeda o site para golpes, quem compartilha, quem usa a máquina infectada, quem recebe e repassa o ganho ilícito)?
9. Como é tratada a divulgação de crimes realizados para recrutamento por facções ou por demonstração de força?
10. Qual é o protocolo de combate a divulgação, venda e entrega de armas, drogas e entorpecentes? Existem casos que possam ser analisados?

#### Sobre os aspectos jurídicos nos crimes via web:

1. Como é resolvida ou tratada a questão da jurisdição em investigações de crimes que são ou podem ser executados em vários locais pelo mundo (Estado/Brasil/Mundo)?
2. Existem acordos de cooperação policial no Brasil para esse tipo de crime? Qual o protocolo adotado para se acionar outras forças da área de segurança?
3. Caso o Brasil venha a aderir, qual a expectativa sobre a aplicação da “Convenção de Budapeste” no referente ao combate ao cibercrime e ao crime digital?
4. A lei 13.964/2019 (Lei Anticrime), que possibilitou a infiltração virtual de agentes policiais para obter dados de conexão e cadastrais de membros de organizações envolvidas com crimes cibernéticos já foi usada em algum caso? Podem ser resumidas para ilustração?
5. Imaginando que a unidade tem participação na Estratégia Nacional de Segurança Cibernética (batizada de "E-Ciber" por meio do decreto 10.222), já existem ações efetivas que possam ser destacadas?
6. Entre os casos de sucesso, existem histórias de ações conjuntas com outras unidades policiais do BRASIL ou do mundo em ações de combate ao cibercrime e crime digital?
7. Tendo as empresas privadas de tecnologia como a Google e Microsoft entre outras, além de ONGs (SaferNet p.ex.) exercido um papel expressivo no combate e sobretudo na denúncia de crimes pela internet, como é a cooperação com a iniciativa privada? Existem protocolos definidos?
8. Existem eventos do tipo “Lei 9099” (Baixo Potencial Ofensivo) que podem ser ou foram resolvidos por Termos Circunstanciados com o escopo dos crimes digitais?