

**PERTANGGUNGJAWABAN TINDAK PIDANA INTERSEPSI DATA
DI INDONESIA**

(Studi Kasus Pada Putusan Nomor 527/Pid.Sus/2020/PN.Smn)

Oleh

Rais Akbar Ridwanullah

E1A018107

ABSTRAK

Perkembangan teknologi di era digital ini dapat memberikan peluang bagi pelaku kejahatan, kejahatan yang semakin merajalela salah satunya adalah kejahatan siber. Intersepsi data termasuk dalam kejahatan *cybercrime*, seperti halnya dalam kasus perkara putusan nomor 527/Pid.Sus/2020/PN.Smn. Maka dari itu tujuan dari penelitian ini adalah untuk mengetahui penerapan hukum pidana dan bentuk pertanggungjawaban terhadap tindak pidana intersepsi data di Indonesia pada Putusan 527/Pid.Sus/2020/PN.Smn. Metode yang digunakan dalam penelitian ini adalah metode yuridis normatif. Hasil penelitian menunjukkan bahwa 1) Tindak pidana Intersepsi data dapat dikenakan Pasal 32, 48, dan 52 ayat (2),(3),(4) UU ITE, dan kasus *deface* di dalam putusan Nomor 527/Pid.Sus/2020/PN.Smn sudah memenuhi unsur tindak pidana intersepsi data yang ada di dalam Pasal 32 ayat (2) jo. Pasal 48 ayat (2) jo. Pasal 52 ayat (2) UU ITE. 2) Pertanggungjawaban tindak pidana Intersepsi data *website* di Indonesia pada Putusan Nomor 527/Pid.Sus/2020/PN.Smn bahwa pelaku peretasan merupakan individu yang cakap hukum, secara sah dan meyakinkan melawan hukum, terpenuhinya unsur pidana Intersepsi data *website*, tidak terdapatnya alasan pembenar dan/atau alasan pemaaf. pasal yang menjerat para pelaku tindak pidana peretasan yaitu Pasal 32 ayat (2) jo. Pasal 32 ayat (2) jo. Pasal 48 ayat (2) jo. Pasal 52 ayat (2) UU ITE.

Kata Kunci: Pertanggungjawaban; Tindak Pidana; Intersepsi Data; Kejahatan Siber.

***Accountability for Data Inteferece Crimes in Indonesia
(Study of Decision Number 527/Pid.Sus/2020/PN.Smn)***

Oleh

Rais Akbar Ridwanullah

E1A018107

ABSTRACT

Technological developments in this digital era can provide opportunities for criminals, crimes that are increasingly rampant, one of which is cybercrime. Data interference is included in cybercrime. As well as the case of decision case number 527 / Pid.Sus / 2020 / PN Smn. so the aim of this research is to understand the application of criminal law and forms of accountability for criminal acts of hacking in Indonesia in Decision Number 527/Pid.Sus/2020/PN.Smn. The method used in this study is the normative juridical method. Research results show 1) The criminal act of data interference can be subject to Articles 32, 48, and 52 paragraphs (2), (3), (4) of the ITE Law, and the deface case in decision Number 527/Pid.Sus/2020/PN.Smn has fulfilled the elements of a criminal act data intervention in Article 32 paragraph (2) jo. Article 48 paragraph (2) jo. Article 52 paragraph (2) of the ITE Law. (2) UU ITE, and the judge's decision in this case was correct, but the decision received by the defendant was too light when viewed from the consequences that had been caused. 2) Responsibility for criminal acts of website hacking in Indonesia in Decision Number 527/Pid.Sus/2020/PN.Smn that the perpetrator of the hacking is an individual who is legally competent, legally and convincingly violates the law, fulfilling the criminal elements of website hacking, there is no justification and/or excuse. Articles that ensnare perpetrators of criminal acts of hacking, namely Article 32 paragraph (2) jo. Article 32 paragraph (2) jo. Article 48 paragraph (2) jo. Article 52 paragraph (2) UU ITE.

Keywords: Liability; Criminal Offence; Data Interference; Cyber Crime.